California Year 2000

Embedded Systems

Program Guide

June, 1998

John Thomas Flynn
State Chief Information Officer
DEPARTMENT OF INFORMATION TECHNOLOGY
801 "K" Street, Suite 2100
Sacramento, CA 95814
Phone: 916.445.5900
Fax: 916.445.6524
www.year2000.ca.gov

California 2000 Embedded Systems Program Guide

Contents

EXHIBITS

TABLES

Acknowledgments

The California Year 2000 Embedded Systems Program represents the efforts of many people. The DOIT wishes to acknowledge the assistance of those who have contributed to the development of this program by participating in the Year 2000 Embedded Systems Task Force and its subcommittees:

Year 2000 Embedded Systems Task Force

Walt Barr	Department of Health Services
Jerry Beaman	Department of Mental Health
John Bowles	Office of Emergency Services
Jack Connell	CTA INCORPORATED
Jerry Cottrell	Department of Finance
Mike Courtney	Department of General Services-Real Estate Services
Joyce Fong	Public Utilities Commission
Toni Frederickson	Department of Forestry & Fire Protection
Angela Garvie	Department of Health & Welfare Agency Data Center
Michael Goble	Department of General Services-Real Estate Services
Susan Hancock	Department of Corrections
Larry Hoffart	Department of Industrial Relations
Bob Jordan	Department of Water Resources
Mike Kanemoto	Department of Justice-Hawkins Data Center
Mike Lucas	DynCorp Management Resources, LLC
John McMahon	California Highway Patrol
John McMillan	Department of Transportation
Leslie Medina	DynCorp Management Resources, LLC
Dana McIntyre	CTA INCORPORATED
Russ Ogata	Sacramento County Public Works
Debra Reiger	Department of Health & Welfare Agency Data Center
Dennis Russell	Stephen P. Teale Data Center
Linda Sanford	Department of Consumer Affairs
Elmer Schau	Stephen P. Teale Data Center
Allan Tolman	Department of General Services-Telecommunications
Doug Yee	Department of Developmental Services

Department of Information Technology

John Thomas Flynn
Ron Ridderbusch
Claudina Nevis
Janice Barnett
Rita Champlion

Section 1: About This Program Guide

The purpose of this document, the *California Year 2000 Embedded Systems Program Guide*, is to communicate the Department of Information Technology's policy, guidance, and reporting requirements for conducting California's Year 2000 program for embedded microprocessor systems.

The primary audience for this guide is the state's agency and department-level personnel who will be responsible for performing the embedded systems risk analysis, site survey, assessment, and remediation activities.

This Program Guide consists of the following six sections:

- **About This Program Guide –** Introduces this Program Guide and describes its contents.

- **California Year 2000 Embedded Systems Program –** Introduces the California Year 2000 Embedded Systems Program; describes the program approach; provides an overview of the program with descriptions of key elements and resources; and defines milestones, timelines, and reporting requirements.

- **California Year 2000 Embedded Systems Management –** Describes high-level project management processes; addresses Year 2000-related risk factors, and provides an overview on risk mitigation activities and contingency planning efforts that support the California Year 2000 Embedded Systems Program.

- **Embedded Systems Categories and Applications –** Describes embedded systems categorizations and provides examples of embedded systems applications.

- **California Year 2000 Embedded Systems Methodology –** Provides a methodology that departments may use to prioritize, survey, assess, and remediate their embedded systems.

- **California Embedded Systems Center –** Describes the services available from the California Embedded Systems Center (CESC) and how to access this on-line service. Specific procedures for using this web-site are available in a separately published document, California Embedded Systems Center User's Manual.

This *California Year 2000 Embedded Systems Program Guide* has been prepared in printed form to facilitate distribution of its contents to relevant personnel throughout each agency and department. It is also available on-line at the DOIT Year 2000 web-site at www.year2000.ca.gov.

Section 2: California Year 2000 Embedded Systems Program

The California Year 2000 Program comprises multiple subprograms focused on particular types of systems, each susceptible to the Year 2000 problem:

Y2K SubProgram	System Type Addressed
California Year 2000 Program Guide	Traditional IT systems.
California Year 2000 Embedded Systems Program Guide	Embedded technology/microprocessor systems/non-IT systems, including telecommunications systems and wide area network infrastructure.
California Year 2000 Program Guide: Desktop Systems	Microcomputers and related network infrastructure, including file servers, local area networks, and desktop computers.
California Year 2000 White Paper: External Interfaces	External Interfaces coordination, synchronization and management issues.

It is important to recognize that differentiation between IT systems, embedded systems, desktop systems and file servers can sometimes be difficult and the boundaries between them blurred. What is important is that each of these systems be addressed under one of the Year 2000 programs. If in doubt as to which subprogram a particular system belongs to, it is better to assess the system twice under two programs than to omit it from either and put it at risk for failure.

2.1 Program Approach

The Year 2000 embedded systems effort will be a challenge to all businesses and government entities. The impact of the Year 2000 date change on embedded systems was underestimated until this last year when industry analysis and Year 2000 efforts performed to date proved that embedded systems are very vulnerable to Year 2000 problems. This vulnerability, combined with the significant quantity and varying complexity of embedded systems in use, and the short time frame to correct deficiencies, requires that departments take immediate action. To meet this substantial challenge, the California Year 2000 embedded systems program approach is to:

1) Implement solid, sustained project and risk management programs;

2) Use a defined embedded systems methodology for accomplishing Year 2000 compliance, and

3) Start now; the deadline date is fixed. Delaying efforts will eliminate remediation options and increase the potential for system failures.

This Program Guide is not intended as a definitive resource providing comprehensive instructions, which if followed, will ensure that the entire department's Year 2000 problems will be removed overnight. The department is advised to carefully read the document and consider the methodology steps in light of the department size and expertise available within the department, and also external resources. The department function and the nature of the processes it uses should be reviewed, along with a thorough evaluation to determine if these involve embedded systems.

2.2 Program Overview

The California Year 2000 Embedded Systems Program is modeled after the California 2000 Program, and is one of its subprograms. The objectives of the program are as follows:

- Fulfill the DOIT's mandate to monitor and oversee California's embedded systems Year 2000 compliance efforts;
- Provide guidance and enabling assistance to state entities in planning and managing their embedded systems Year 2000 projects;
- Promote sharing of information; and
- Leverage inter-departmental resources to achieve economies of scale across state enterprises.

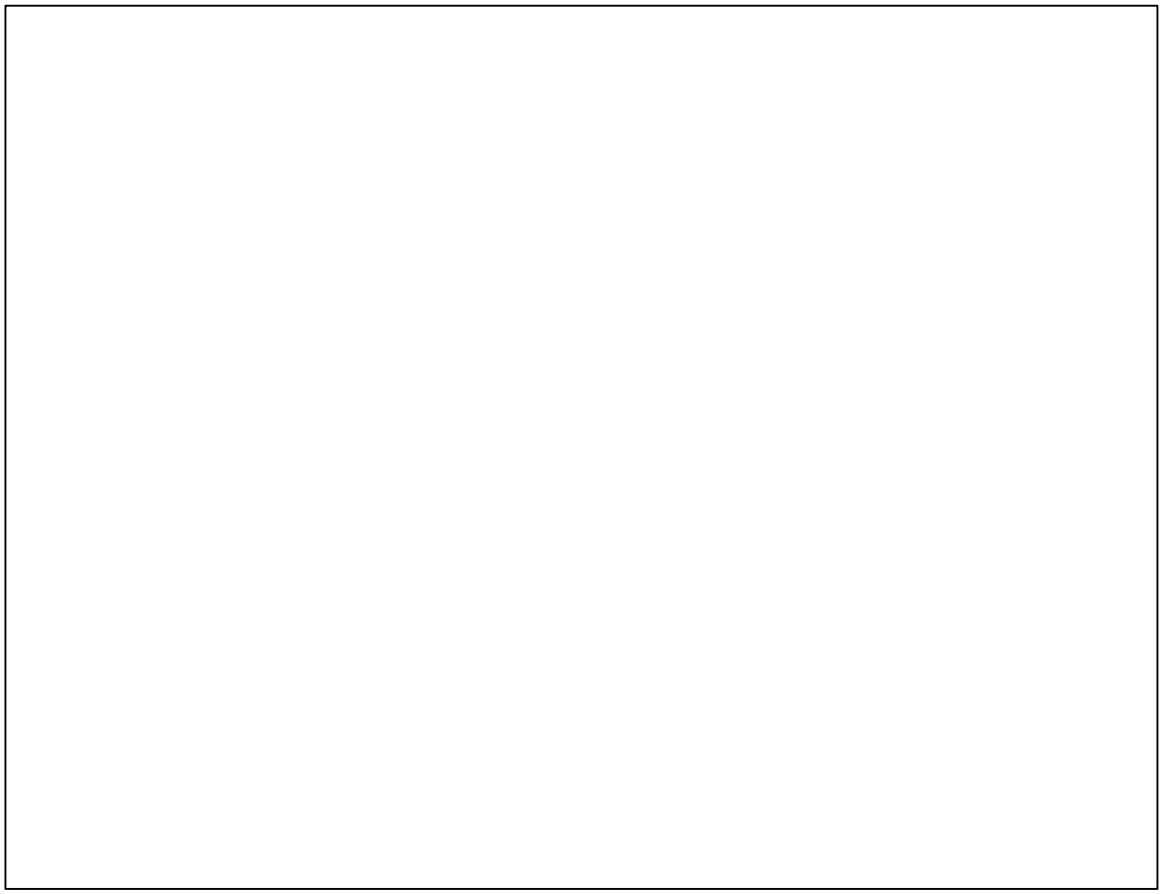


Exhibit 2.2-1. California Year 2000 Embedded Systems Program

The following sections describe the program components illustrated in Exhibit 2.2-1, California Year 2000 Embedded Systems Program.

2.2.1 California Embedded Systems Task Force

The DOIT has established the California Embedded Systems Task Force to assist in developing and leading California's Year 2000 Embedded Systems Program. It is a forum of selected personnel empowered to represent their agencies' points of view in the development and operation of the program. The Task Force will assist the DOIT by reviewing plans and progress, making recommendations, contributing new ideas, and communicating the program to their agencies.

2.2.2 California Year 2000 Embedded Systems Methodology

The methodology described in Section 5 of this Program Guide was developed from best practices used in the private sector and those currently in use in whole or in part by some California departments. It is offered as a baseline methodology that departments may use 'as-is' or tailor to better meet their departmental needs.

2.2.3 California Embedded Systems Center

The California Embedded Systems Center (CESC) is a pilot program established to provide technical assistance and serve as a repository for embedded systems Year 2000 compliance data. It is available to all State of California departments on a trial basis and may become available to other government entities. The embedded systems web-site, *www.cesac.com*, has been constructed to support departments in their interface with the CESC. The CESC can also be contacted at 800.433.1757. See Section 6 for more details on this service.

2.2.4 Department of General Services and Vendor Coordination

The California 2000 Office worked with the Department of General Services (DGS) to facilitate the development of Year 2000 contract language to be incorporated in all model contracts.

2.2.5 California 2000 Web-Site

The California 2000 Web-Site, www.year2000.ca.gov, has been created to foster information-sharing with all departments. This site provides specific correspondence, management memos, and other relevant information about the Year 2000, as well as a forum where users can post their Year 2000 questions and receive answers from other users. This site allows state government users to share information so all departments can leverage best state practices.

2.2.6 California 2000 Embedded Systems Reporting Requirements

The Year 2000 Embedded Systems reporting requirements have been developed to assist departments in providing embedded systems data needed for statewide reporting. The data provided will meet the DOIT's mandated reporting requirement for Year 2000 Quarterly Updates to the Legislature and Administration.

2.3 Program Timeline and Reporting Requirements

The following chart depicts major milestones and reporting requirements in California's Year 2000 Embedded Systems Program.

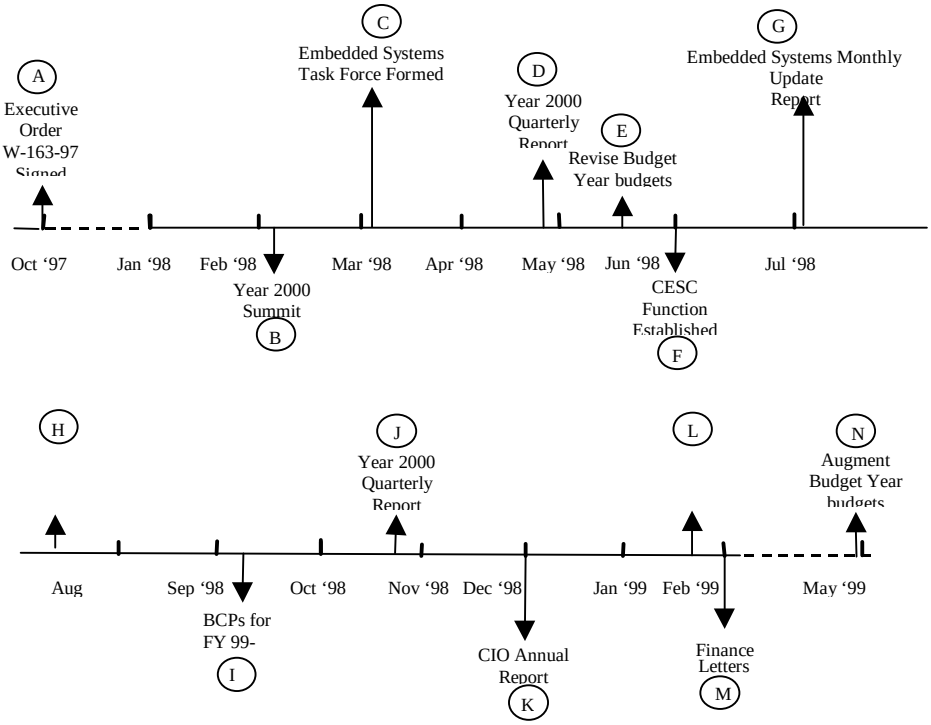


Exhibit 2.3-1 California Year 2000 Embedded Systems Program Reporting Timeline

The following is a brief description of the major milestones and reporting requirements illustrated above.

A) **Executive Order W-163-97 Signed**: Governor Wilson issued Executive Order W-163-97 directing the DOIT to continue coordinating the State's Year 2000 Program and specifically directing the DOIT to address embedded microchip Year 2000 issues. (See Appendix A.)

B) **Year 2000 Summit:** On February 19, 1998, the DOIT sponsored the California Year 2000 Intergovernmental Summit to address a number of Year 2000 issues including embedded systems.

C) **Embedded Systems (ES) Task Force Formed:** On March 4, 1998, the DOIT established, and on March 17, convened the first meeting of the Year 2000 Embedded Systems Task Force to assist in developing and leading the California Year 2000 Embedded Systems Program.

D) **April 1998 Year 2000 Quarterly Report:** On April 27, 1998, the DOIT issued the fourth California Year 2000 Progress Report.

E) **May Revision of General Fund Revenues and Expenditures for Fiscal Year (FY) 98-99:** This is the last opportunity departments have to augment their Budget Year budgets. Departments should plan budgets for embedded systems risk analysis, site survey, assessment, and remediation planning and execution.

F) **California Embedded Systems Center Established as a Pilot Program:** By July 1, 1998, the DOIT is scheduled to sponsor and establish a repository function for Embedded Systems (ES) compliance data, initially accessible to state departments at no charge.

G) **Embedded Systems Monthly Update Report (MUR):** This is the first Embedded Systems Monthly Update Report incorporating Year 2000 embedded systems status data. This report will include results from the departments site survey, assessment and remediation activity. Departments are scheduled to submit this report to the DOIT by July 31, 1998.

H) **July 1998 Year 2000 Quarterly Report:** The DOIT is scheduled to issue another California Year 2000 Progress Report in late July, reflecting initial data from departments on their embedded systems progress.

I) **BCPs Due for FY 99-2000:** Departments submit their FY 99-2000 Budget Change Proposals to the Department of Finance.

J) **October 1998 Year 2000 Quarterly Report:** The DOIT is scheduled to issue another California Year 2000 Progress Report in late October, continuing to incorporate embedded systems progress data.

K) **CIO Annual Report for 1998:** In December 1998, the DOIT will issue the CIO annual report, which will include embedded systems Year 2000 status.

L) **January 1999 Year 2000 Quarterly Report:** The DOIT is scheduled to issue California's Year 2000 Progress Report in late January, incorporating updated remediation planning data.

M) **Finance Letters for 98-99 Due:** In February 1999, departments identify changes to their Budget Year budgets to the Department of Finance. Departments may need to use their updated Embedded Systems Remediation Plans as justification for Year 2000 budget augmentation.

N) **May Revision of General Fund Revenues and Expenditures for FY 99-2000:** This is the last opportunity departments have to augment their Budget Year budgets. Departments may consider budget augmentation for embedded systems remediation based on estimated costs in the most recent remediation plan update.

2.3.1 Legislative Reports

On a quarterly basis, the DOIT is required to report the status of the State's Year 2000 efforts to the Legislature. The report includes progress and level of compliance with the Year 2000 program, identification of programs at risk, and updated estimates of cost. The DOIT will expand the quarterly report to address embedded systems.

2.3.2 Department Reporting

Existing monthly departmental Year 2000 reports will be expanded to capture embedded systems data. Departments will begin reporting embedded systems progress to the DOIT on July 31, 1998. Specific reporting instructions will be provided with the July 1998 Embedded Systems Monthly Update Report distributed by the DOIT to departments.

Section 3: California Year 2000 Embedded Systems Management

The California Year 2000 Embedded Systems Program will require consistent application of effective management processes throughout the Year 2000 effort. In addition to presenting a daunting technical challenge, compliance activities will require a significant coordination effort.

Risk management is absolutely necessary to minimize potential Year 2000 system failures and address due diligence requirements. Risk management efforts include the planning and execution of risk mitigation activities and development of contingency plans to avoid or minimize the effects of a system failure.

3.1 Project Management

Successful execution of the Year 2000 embedded systems effort is not only a technical challenge, but also a considerable management challenge for all businesses and government entities. It will require the coordination and tasking of personnel and resources to perform the Year 2000 embedded systems methodology activities (risk analysis, site survey, assessment, and remediation, if necessary) within the constraints of a relatively short and inflexible schedule, and limited funding and resources. "Buy-in" from top-level management and staff is needed to ensure that Year 2000 projects are given the time and attention necessary to be successful.

The following project management activities provide the needed support to meet this significant challenge:

Dedicated embedded systems (ES) Year 2000 project manager and team with clearly defined roles, responsibilities and expectations;

Thorough planning;

Cost/schedule development and status monitoring;

Well-defined configuration, data and quality assurance controls;

Timely, effective communication with all involved personnel, including personnel external to the department.

***Dedicated Year 2000 project manager and team*.**

- Designate a departmental ES Year 2000 project manager who has the responsibility and authority to lead, direct, monitor, and report to management and the DOIT from a department-side perspective. This person should have a strong knowledge of the department functions and working knowledge of embedded systems. Additionally, the department ES Year 2000 project manager should have organization and communication skills necessary to effectively develop and communicate department plans, methodology, and standards.

- Identify the skill mix and knowledge base (management, functional, technical) required for the dedicated ES Year 2000 project team. Management skills will be needed for planning and executing activities, making assessments, prioritizing activities, and monitoring progress. Technical skills will be needed to address the relevant system hardware and software. Department functional knowledge will be beneficial in identifying high impact systems and the departmental-specific personnel and processes to assist in performing Year 2000 activities most effectively.

- Define and communicate project team roles, responsibilities, and expectations. This will help minimize misinterpretation, conflict, and redundancy.

- Train all members of the project team on the ES Year 2000 methodology, and the management processes and procedures that will support the Year 2000 activities. This will ensure that the Year 2000 activities are well understood and performed consistently.

- In the performance of ES Year 2000 methodology activities, large departments or those departments with large quantities of embedded systems may find it beneficial to organize their team into groups according to system type (i.e. facilities and medical systems). This will facilitate department Year 2000 efforts by developing team 'subject matter experts' who will be able to more quickly perform activities--having overcome the learning curve on particular groups of systems.

Thorough Planning. Thorough planning will require considering and addressing many factors. These factors include: current and future embedded systems upgrades and replacements; size of the department's Year 2000 effort and how many/type personnel, consultants, and tools will be necessary to support it; cost and schedule requirements and constraints, and interdependent activities. Planning needs to be thorough, but flexible. Knowledge will be gained through the performance of each activity (lessons learned); this will inevitably impact plans and require reassessment of plans, processes and priorities that support the ES Year 2000 activities.

Cost/Schedule Development and Status Monitoring. The department's Year 2000 project office needs to develop ES Year 2000 budgets, track costs, and prepare and update departmental Year 2000 schedules. These will be used to report the status of the department ES Year 2000 progress, highlight potential problems, and determine future resource requirements. The DOIT has established reporting requirements for departments to document the current status of their Year 2000 embedded systems progress. Detailed procedures for providing this data will be provided with the June ES Monthly Update Report. The ES milestone schedule is discussed in Section 2 of this guide.

Configuration/Data/Quality Assurance Controls. Implement configuration management and quality assurance processes and procedures. These will be necessary to control and document system configurations to ensure correct system

identification, eliminate the possibility of reintroducing non-compliance in successfully tested systems, and reduce inefficiencies.

Develop and implement standardized data management processes for collecting data throughout the ES Year 2000 program. This helps minimize the possibility of misinterpreting or leaving out critical information on a system, reduces redundancy of effort, and simplifies status reporting.

Designate quality assurance personnel to assist in the development of standardized processes and procedures, to monitor and perform audits to ensure their correct implementation, and to assist in developing standards for and observing compliance testing.

In addition to collecting system data and Year 2000 progress, information about issues, discrepancies, actions, and impacts is important to document for circumstances where the department may need to prove that it took all reasonable precautions and exercised due diligence.

Effective Communication. Communication is essential; plans, schedules, responsibilities, requirements, and problems need to be understood by all personnel involved in the Year 2000 effort. It is absolutely necessary that communication and coordination occur beyond the department line and throughout the Year 2000 program. Because nearly every aspect of embedded systems is impacted, there are many opportunities for failure outside of a department's direct control. Year 2000 problems are liable to affect a large proportion of the individuals in the department, either because they would be at some risk if there were a failure, or because the need to investigate will cause them additional work or disrupt their work routines

Success in investigating and identifying date sensitive systems will depend on obtaining widespread cooperation from department employees, relevant suppliers, vendors, and consultants. For these reasons, it is necessary to ensure that employees at all levels are:

1. Made aware of the problem;

2. Asked for information and cooperation;

3. Warned of possible disruptions to operations and services; and

4. Advised of changes that might affect them.

Even though each system may be different in design or function, the process of achieving compliance is common to everyone involved in the Year 2000 effort, and one person's efforts could benefit many if shared. Shared information may include lessons learned, issues, and compliance status of a major supplier/interface.

3.2 Risk Management and Contingency Planning

The embedded systems Year 2000 program is very susceptible to risk due to both internal and external factors, including the inflexible nature of the schedule, the volume of embedded systems in existence that may need remediation, limited resources, legal issues and liability, operational impact, and system interdependencies. It will be necessary to evaluate the impact of failure(s), the probability of occurrence, and to develop risk management activities and contingency plans to address and mitigate these risks.

Risk Management Activities. These are activities that should be performed throughout the ES Year 2000 effort. The California Year 2000 Embedded Systems Methodology contains risk management activities within each phase: e.g., risk analysis, execution of standardized site survey processes, compliance testing, risk evaluation, contingency planning, and system monitoring. The utilization of this methodology, together with the consistent application of the management processes and procedures defined in this Guide, will significantly support departments in managing their department Year 2000 risk.

Contingency Planning. Contingency plans for ES Year 2000 systems are the plans for action in the event that a system failure occurs. The purpose of these plans is to avoid or minimize the impact of failure by ensuring a well-thought out plan for immediate implementation. Contingency plans are required for high-priority/high-impact systems. They address both failures that are within the control of the department, as well as those that are beyond the control of the department such as power failures or interdependent systems.

Development of detailed contingency plans will occur concurrently with remediation planning activities performed in the fourth phase of the California Year 2000 Embedded Systems Methodology (see Section 5.4).

Section 4: Embedded Systems Categorizations and Applications

This section contains relevant categorizations and applications of embedded systems to assist the reader in understanding the complexity of the embedded system problem.

The simplest embedded systems are capable of performing only a single function or set of functions to meet a single predetermined purpose. In more complex systems, the functioning of the embedded system is determined by an application program that enables the embedded system to be used for a particular purpose in specific application. The following are categories or levels (from lowest to highest level) of embedded systems.

1. **Individual microprocessors**: may be found in small devices such as temperature sensors, smoke and gas detectors, and circuit breakers. The supplier of the device has principle responsibility for design and operability, provided that the device is used for the purpose for which it was supplied. It is unlikely that they will be date sensitive; however, if they are, it will not be evident until after the date change. Determination of date sensitivity will require testing.
2. **Microprocessor assemblies with no timing function**: may be found in flow controllers, signal amplifiers, position sensors, and valve actuators. It is unlikely that these will be affected; however, their internal operation may depend on a clock provided by a timing device that may have Year 2000 problems.
3. **Subassemblies with timing function**: are devices such as switchgear, controllers, telephone exchanges, lifts, data acquisition and medical monitoring systems, diagnostic and real-time control systems. They might be local elements in a larger system to which they pass data collected by their sensors. They may incorporate a PC and may involve some kind of database. The Year 2000 problem may affect their systems, application software, the database, and the networks and data transmission systems they use to communicate with the larger system.
4. **Computer systems used in manufacturing or process control**: relates to cases where a computer is connected to machinery in order to control it. In such systems, the computer is used for overall control and monitoring, rather than for direct control of individual devices within it.

Process control systems may be linked with business systems (using sales figures or stock levels to determine order or production quantities). In many cases, two distinct and separate subsystems may operate in a single system. In a control and safety system, the primary subsystem controls the process so that the various devices in the system operate and interact correctly to produce the product. The safety subsystem reduces the risk of malfunctions that might affect the safety of individuals or harm the environment.

Embedded systems are affected by Year 2000 problems in the same way as commercial data processing systems. Four common elements with possible data sensitivity are contained in a PC-based system: the date and version of the BIOS and CMOS, the date and version of the operating system, the application and how it derives its internal time structure, and the firmware (applications software contained in hardware created for a particular purpose).

Examples of embedded system applications are as follows:

Manufacturing and Process Control	
Manufacturing plants	Bottling plants
Water and sewage plants	Automated factories
Power stations	Test equipment for control system development, maintenance and testing
Power grid systems	Oil refineries and related storage facilities
Construction	
Surveying and locational equipment	Construction plant
Transportation	
Airplanes, trains, automobiles, buses, marine craft	Radar systems
Fuel services	Traffic lights
Air traffic control systems	Ticketing systems/machines
Signaling systems	Car parking and other meters
Buildings and Facilities	
Electrical supply: supply, measurement, control, protection	Lifts, elevators, escalators
Backup lighting and generators	Security systems
Fire control systems	Safes and vaults
Heating and ventilating systems	Door locks
Domestic Services	
Catering	Cleaning
Communications	
Telephone exchange	Satellites and Global Positioning Systems (GPS)
Cable systems	Data switching equipment
Telephone switches	
Office Systems and Mobile Equipment	
Telephone systems	Time recording systems
Faxes	Mobile telephones
Copiers	Still and video cameras

Banking , Finance, and Commercial	
Automated teller systems	Point of sale systems
Credit card systems	
Medical Diagnostics, Monitoring, and Life Support	
Heart defibrillators	Pharmaceutical control and dispensing systems
Pacemaker monitors	X-ray equipment
Patient information and monitoring systems	Electrocardiograph and electro-encephalograph equipment

Section 5: California Year 2000 Embedded Systems Methodology

The application of a defined methodology is a key factor in exercising due diligence in the management of Year 2000 issues. California's Year 2000 Embedded Systems Program has developed a project methodology derived from best practices in use by the private sector and some state departments. This methodology provides an orderly, standardized process to analyze system risk, conduct site surveys, assess Year 2000 compliance, and remediate non-compliant systems. State departments may use the methodology in its present form or tailor it to better address their specific needs. The *California Embedded Systems Center (CESC)* web-site, **www.cesac.com** is an on-line, easy-to-use service that provides the user with step-by-step methodology instructions; it is a suggested resource for all departments to use. Section 6, California Embedded Systems Center, provides additional information on the capabilities of this resource for department use.

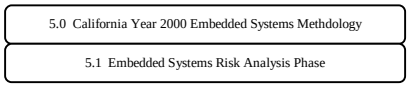
The Embedded Systems Methodology consists of four major phases: risk analysis, site survey, assessment, and remediation. While these steps are sequential for individual systems, an organization may be involved in different phases on different systems simultaneously, and not all systems will require all the phases. Table I, Embedded Systems Project Overview lists the Year 2000 project phases and the approximate cost percentage and time frames, depicted as estimates only. Actual cost percentages and time frames will vary by department and by systems within a department, depending on specific system configurations, level of staffing, approaches, and solutions.

Table I. Embedded Systems Project Overview

Year 2000 Embedded Systems Methodology Phase	Approximate Project Cost (%)	Approximate Time Frame
1. Risk Analysis	5%	1-2 Weeks
2. Site Survey	15%	1-2 Months
3. Assessment (Vendor Management, Compliance Determination, Risk Evaluation, Remediation Strategy)	15%	2-3 Months
4. Remediation (Planning, Installation, Testing, Monitoring)	50%	6-12 Months
Management (Planning, Oversight, Communication, Reporting)	15%	Throughout Project

Details of each phase are described in the following subsections and depicted in Exhibit 5-1 California Year 2000 Embedded Systems Methodology on the next page.

5.1 Embedded Systems Risk Analysis Phase



The purpose of the Risk Analysis Phase is to identify, categorize, and rank embedded systems in preparation for effectively conducting site survey and following phase activities. Results of this effort will provide an initial estimate of the number of departmental embedded systems, and a system ranking which will be used to first focus efforts on the highest impact systems. This is an initial determination; through performance of subsequent activities, system categorization and ranking may change.

Categorize Risk. Departments should first concentrate on identifying critical embedded systems, defined as those contributing to department core missions, programs, or support services. These embedded systems are to be categorized[1] as follows:

- **Category 1 - Health and Safety:** where the loss or degradation of these systems could jeopardize the health and safety of California State employees or the public, or the safety of State property or private property.
- **Category 2 - Environmental Impact:** where the loss or degradation of these systems could negatively impact the environment within the State of California.
- **Category 3 - Operational Impact:** where the loss or degradation of these systems could negatively impact the ability of a department to perform its missions.
- **Category 4 - Public Confidence:** where the loss or degradation of these systems could cause the public to lose confidence in the State's government.
- **Category 5 – Other:** systems that are not categorized above.

Category Ranking. To further filter and focus the site survey efforts on the most crucial systems, performance of a preliminary ranking of systems within each category according to level of risk is recommended. The levels of risk are defined as high, medium, and low. This ranking will be especially helpful for those departments that have a significant number of embedded systems, and for those departments that have systems which do not fall under the first two categories of risk impact (health and safety, environmental), but where system failure could have significant impact on their core department functionality.

An example of the results of this risk analysis effort is shown in the following table and a template is included in Appendix C.

[1] In instances where a system could be categorized in more than one category, assign it to the highest category which applies.

Table II. Embedded Systems Risk Analysis Report

Department Name:

Risk Category		Category Ranking			
No.	Title	Total Systems	High	Medium	Low
1	Health, Safety				
2	Environment				
3	Operations				
4	Public Confidence				
5	Other				
Total Embedded Systems					

All embedded systems should be included in this risk analysis activity, including systems that are scheduled for replacement or elimination. Should the change not occur as planned, the likelihood of missing a system is thus reduced.

Planning. After performing this risk analysis activity, the department Year 2000 project manager should then meet with the designated Year 2000 business and functional leads, facility managers, and operation and maintenance personnel/ contractors to organize the site survey activities to follow. Plans should address:

1. The skill set and number of personnel needed to perform the site survey effort;
2. How the effort will be divided (i.e., business area, function, or facility);
3. What systems will be addressed first (using risk analysis results);
4. Schedule requirements, and
5. The standardized forms that will be used to collect information.

It is critical that the department uses standardized formats and implements data management procedures for control and maintenance of data. This will provide consistent and efficient reporting and minimize repetition of effort and data loss.

Lessons Learned:

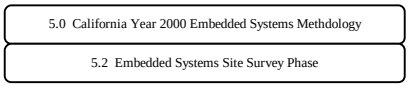
Lessons learned on previous state department site surveys should be considered when planning current site survey activities, and include the following observations:

- Distribute survey forms and instructions to all survey team members in advance of the effort. Discuss the instructions and the importance of gathering as much of the data listed on the forms as possible, with special focus on the required field data (system name, manufacturer/vendor, model or serial number, and point of contact information). The required survey data is key to performing vendor management activities--missing data will delay further activities and necessitate that personnel revisit the facility or contact the facility/system point of contact for information. At times the model/serial number may not be readily available; in

these cases the point of contact information will be considerably useful to the personnel performing the vendor management.

- Some departments have systems that they do not want to disclose in normal site survey activities—provisions need to be made to ensure that these systems are addressed under the Year 2000 program.
- Survey efforts were most effectively performed with two-member teams: one to locate information (i.e. manufacturer model number) and one to record the information.
- Coordinate site survey activities with the facility coordinator and subject matter experts (SMEs) well in advance. Be sure to ascertain SMEs schedules, as they may often be required to perform their normal duties in addition to working with survey teams, and consider that their schedules may vary from the normal 8:00 a.m.-5:00 p.m. work schedule. Also keep in mind that access to certain facilities may require advanced background checks.

5.2 Embedded Systems Site Survey Phase



The purpose of the site survey is to gather/document essential information about the department's embedded systems. It is crucial to develop a comprehensive, system-wide understanding of the number, type, location, and configuration of relevant components within the embedded systems environment, including internal and external interfaces that utilize or display time/date information. This data is the basis for all subsequent Year 2000 activities, and additionally will be used for planning the next phases and determining the resources, costs, and schedules necessary to perform Year 2000 efforts. Information gathering will likely occur throughout the Year 2000 project as more in-depth research unveils unknown systems, interdependencies, and additional risk factors. Listed below are the types and examples of information to be gathered. Templates of the site survey forms are included in Appendix D.

It should be noted that it might not be possible to gather all system information listed below during the survey activity. However, in order to perform effective vendor management (Phase 2), it is absolutely necessary to gather the manufacturer/vendor name, model or serial number and point of contact for the system involved. This will lessen the need to re-survey systems which might delay in subsequent Year 2000 activities.

Department and Facility Data includes department name, facility name and address, and facility owner[2] with telephone number.

Configuration Data defines the system hierarchy, including the subsystems and components, manufacturer(s) or vendor(s) names, the model number(s) and serial number(s), and the population (quantity of identical items).

The system hierarchy may consist of a single device connected to a power source; a complex system comprising several embedded systems built and maintained by one vendor; a system of several embedded systems built by several different manufacturers acquired by a vendor who provides connections, interfaces, or modifications to create a system to meet customer requirements (system house or integrator); a system of several embedded systems developed and maintained within the department; or a custom built system—all of which perform one or more specific functions.

Because a system can be comprised of many components, and each component could have compliance problems that could negatively impact the ability of the system to function properly, it is necessary to record all system information, even for those that are built and maintained by one vendor. This information will be especially useful in cases where the compliance of the system in question is uncertain; the vendor has not

[2] The state/department may own the facility or it may be leased. This information has significance when a leased building has a facility-related system, such as a building security system, that requires remediation actions. Efforts like this will require coordination with the leasing company and the Department of General Services.

provided a certification of compliance for the system; and based on the system's risk category, a decision was made to perform compliance testing. Additionally, there may be cases where individual components have been upgraded by operation and maintenance personnel without vendor notification. Identification of the entire system configuration, including defining system interdependencies, is one more step towards managing risk and ensuring successful Year 2000 system compliance.

Interdependencies are the internal and external interfaces that support the embedded system in question. They may include network system components such as servers, routers, and bridges that support the transport of data from one system to another, power systems such as utilities[3] (i.e., gas, electric) and power backup systems such as uninterruptable power supplies, or other systems (within or outside the department) that provide input into the system or to which the system provides data outputs.

Interface information that should be gathered and documented includes:

- the name of the interfacing system;
- a general description of the function provided by the interface;
- the date sensitivity of the interface;
- system Y2K compliance status; and
- the point of contact and phone number.

Interface compliance is a significant issue in the Year 2000 embedded systems effort. Just one non-compliant interface can severely impact the operation of an entire system and the success of a department to meets its Year 2000 goals. To mitigate this risk, it is advisable to communicate frequently with the owners of the interface about the current conversion status, work together towards solutions, *and* develop contingency plans to address possible non-compliance.

Risk Category is the same categorization of systems made during the risk analysis phase (i.e., Health and Safety, Environment, Operations, Public Confidence, Other). Refer to Section 5.1 for definitions of each category.

Category Ranking is the ranking of systems (high, medium, low) within each risk category made during the risk analysis phase.

[3] **Note:** For major interface suppliers common to all departments—such as utility companies—it is advisable to appoint one focal point of contact, as this will lessen the workload and the likelihood of misinterpretation of information.

Date Sensitivity identifies the surveyor's current knowledge of the system's date-sensitive characteristics. Embedded systems' date sensitivity may be identified by considering whether the systems perform time-related functions or possess time-related characteristics. Failures may occur in systems that:

1. implement a timed control sequence operated on a timed basis (i.e., five minute cycles);
2. shut down unless a maintenance cycle is adhered to;
3. produce regular (i.e., hourly, daily, weekly) reports;
4. report/handle timed events and alarms;
5. calculate totals over time;
6. calculate averages, rates, or trends;
7. rely on external timed data (i.e., Inter-Range Instrumentation Guide [IRIG] for system synchronization);
8. rely on external geographical Global Positioning Satellite (GPS) data;
9. use or produce time-stamped data;
10. maintain historical state-of-system data.

It is also important to keep in mind that a system may have date sensitivity even if it does not involve any of these functions or characteristics, such as the system that has no timing function but depends on a clock for internal operation.

Table III shows a date-sensitivity matrix by risk category and ranking to assist in determining whether to continue on to the next activity for the particular embedded system under review.

Table III. Embedded Systems Date Sensitivity Matrix

		Date Sensitive?		
Risk Category	**Risk Ranking**	**If Yes:**	**If No:**	**Unknown:**
Health/Safety	H or M or L	AR	NFA	AR
Environment	H or M or L	AR	NFA	AR
Operations	H or M or L	AR	NFA	AR
Public Confidence	H or M or L	AC	NFA	AC
Other	H or M or L	AC	NFA	AC

KEY:
H = High
AR = Assessment Required
M = Medium
AC = Assessment Subject to Cost and Schedule Constraints
L = Low
NFA = No Further Action

Date Functionality addresses how the date is used in the embedded system. If the system is determined to have date sensitivity, it is then important to identify, if possible, its date source (is it internally or externally supplied?) and how it utilizes the date for system function. System date utilization is categorized as follows:

- passive date utilization
- active date utilization
- cyclical (regular intervals—without consideration of day-in-year, week-in-year)

Passive date utilization includes systems with date stamping for recording events such as ticketing systems or surveillance systems that time tag an event but do nothing other than log it. Systems in this category will *generally* experience less serious Year 2000 failures (i.e., a report has an incorrect date); however, for surveillance/security systems that monitor and time-tag events, an incorrect date on a video could have more serious legal consequences.

Active date utilization includes systems that use the date for process control. Building control and alarm systems are examples of active date utilization systems. These systems use time of day and date to calculate when to activate process/control equipment. The building control system may have a date/time function that is programmed to turn off the central air conditioning system between 6:00 p.m. and 8:00 a.m. Monday through Friday and all day on weekends and holidays. Systems with active date utilization have the potential for greater Year 2000 failure impact: inconvenience, damage, total operation failure, injury, or death.

Cyclical time utilization is not *date* driven, although on the surface it may seem to be. An example of a cyclical time-based system is a typical automated irrigation system that has *day* and time sensitivity. The sprinkler system uses a twenty-four hour clock/seven day cycle that it uses to control when the water supply is turned on and off. When the seventh day is over, it recycles back to the first day to restart the cycle. The embedded system, in this case, although having day/time sensitivity does not perform any day-in-year calculations (date); therefore, it will not have Year 2000 compliance issues.

Much of this information may be difficult to determine in the site survey phase and will require investigation during the vendor management and compliance determination activities.

Failure Impact describes the impact of failure due to system non-compliance.

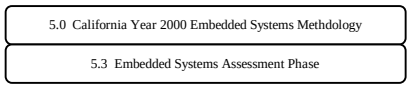
Perform Quality Check of Survey Forms

Upon completing each day's site survey activities, it is very important for the survey team to review the data forms for required field information and understandability-missing information and clarity can easily be obtained at the time of the survey.

Unclear or missing required field data cause additional workload and can delay subsequent Year 2000 activities.

The California Year 2000 Embedded Systems site survey phase is a standardized process for gathering embedded systems data. Results of this effort will provide the Year 2000 department project manager with information needed to proceed into the next phase. The assessment phase will provide additional data towards evaluating different remediation strategies and risk, and estimating cost, resource, and time requirements necessary to address the department's Year 2000 problem.

5.3 Embedded Systems Assessment Phase



This phase comprises the vendor management and compliance determination activities that help determine if, and how, the system will be impacted by the Year 2000 problem, and the development of the most effective means to solve the Year 2000 problem for the particular system. Exhibit 5.3-1 summarizes the embedded systems assessment phase activities.

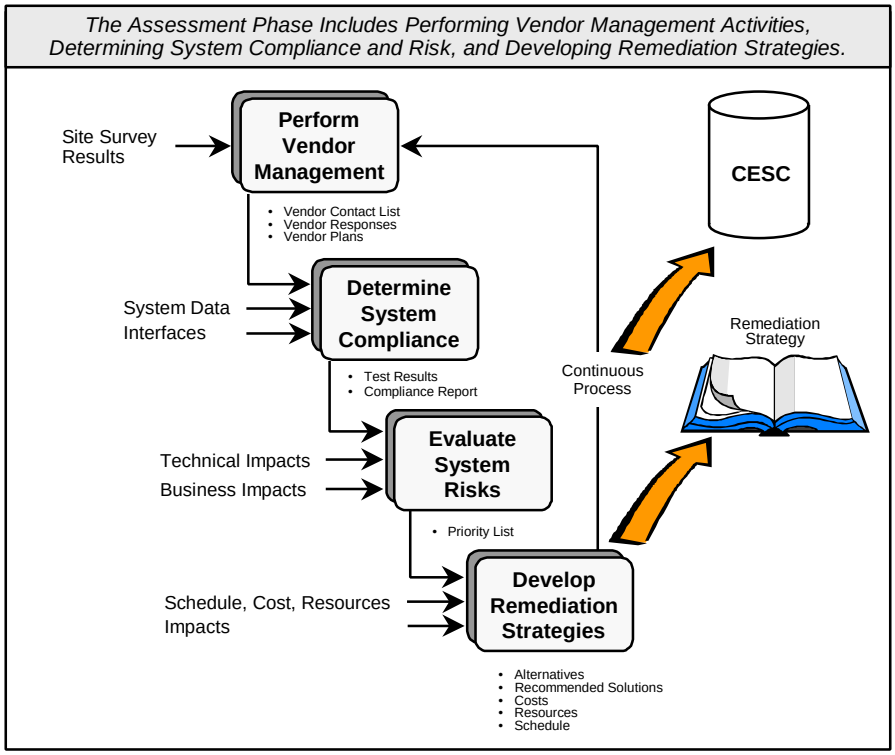
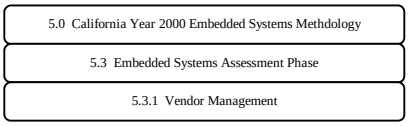


Exhibit 5.3.-1 Embedded Systems Assessment Phase Activities

5.3.1 Vendor Management



Vendor management involves identifying sources of Year 2000 compliance data for an embedded system including the correct manufacturer of the system, vendor point of contact, plans, schedules, compliance statements, and testing data, if available, and any additional data on the system that will support the assessment effort. This is a time-consuming effort. Prior experience indicates that not all vendors will respond quickly, if at all; some embedded systems vendors may no longer exist. Vendors may commit to future dates for Year 2000 compliance. It will be necessary to follow-up and verify that these commitment dates are being met. Frequent vendor contact or additional research will likely be necessary to obtain system configuration identity and level of compliance. An overview of the vendor management tasks is shown in Exhibit 5.3.1-1.

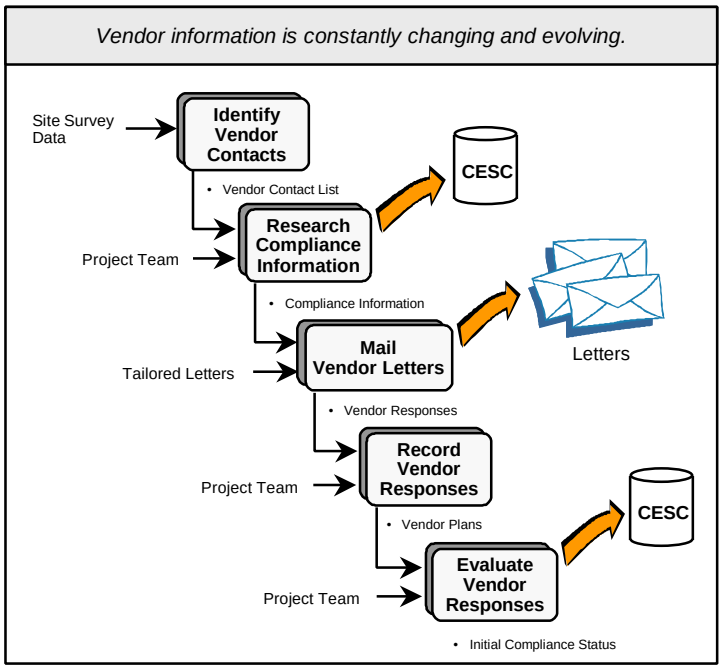


Exhibit 5.3.1-1 Vendor Management Activities

Review. This process starts out with reviewing the site survey results and determining if any critical information is missing, such as model number or manufacturer/vendor name. Having all the information up-front will make the vendor contacts much more effective and less time consuming.

Vendor Contacts. Identify contact names, address, and phone number for each vendor. This is accomplished by various means. Initial sources might be the maintenance or facility engineer, or the responsible system engineer. Other sources are the telephone yellow pages, internet sites, and maintenance manuals. Contact the vendor by telephone or e-mail; inform them of the survey effort and its purpose; verify the correct name, address, and point of contact for the system involved; and inform the vendor that they will be receiving a vendor survey letter and the need for their timely response.

In some cases, particularly for recently procured equipment, the system may already be Year 2000 compliant, or the vendor has included provisions for achieving compliance. This information can usually be found in the system's user or maintenance manuals, in press releases, or through the individual vendor web-site (Internet). It is important to make a copy of the vendor's statement, and for critical systems, it would be advisable to contact the vendor and verify that a specific system implementation is compliant. It should be noted that some vendor claims of compliance will change throughout the department's Year 2000 process, due to further testing and analysis; additional checking of the vendor web-site is recommended.

In cases where the vendor no longer exists or the system is custom built, check for system documentation such as planning documents, system requirement/design specifications, test-related documents, drawing packages, and maintenance manuals. These should describe how the system functions and contain information such as data flow diagrams, input/output specifications, operational cycles, initial start-up and restart features, interfaces, and test and maintenance procedures. This documentation will be especially useful during compliance testing.

Vendor Letters. The vendor survey letter requests *written* confirmation of Year 2000 compliance status, plans for supporting the system if it is not compliant, and the cost for any upgrades or retrofits needed to accomplish compliance. The letter also specifies a deadline for the vendor's response. Anticipate that response may be slow; vendors are being contacted every day about compliance issues of their products. Past experience indicates that sending an e-mail letter, wherever possible, together with a regular mailed letter, is more effective than just mailing the vendor survey letters.

A copy of a sample vendor letter is shown in Exhibit 5.3.1-2, which can be tailored as needed to fit the department environment and requirements. It is suggested that departments work with the DOIT to review and approve the letter before it is issued because laws and guidelines regarding contractual obligations, software licenses, and product warranties vary.

Exhibit 5.3.1-2 Sample Vendor Letter

Year 2000 VENDOR SURVEY

To: _____

Attention: _____

Reference: _____

For the purposes of this survey, "Year 2000 Compliant" or "Year 2000 Compliance" means: *The product(s), when used in accordance with its specifications and documentation, shall:*

- Identify and process date and time date without causing any processing interruptions, abnormal terminations, or change in performance level, characteristics, or functionality of the product;

- Identify, process, and manipulate all date and time date related functions correctly (including leap year calculations, day-in-year calculations, day-of-week calculations, and week-of-the-year calculations);

- Correctly handle date and time related data before, on and after January 1, 2000, including but not limited to accepting input, providing date data output, and performing ongoing operations on dates and portions of dates, including but not limited to calculating, comparing, and sequencing of dates; and

- Correctly store and provide output on all date and time date in a manner that is unambiguous as to century.

1. ❑ The product identified herein is Year 2000 Complaint and will function as specified from the date of purchase and after without interruption attributable in whole or in part to a Year 2000 Compliance error or deficiency.

2. ❑ *The product identified herein is <u>not</u> Year 2000* Compliant, *but will be made Year 2000 Compliant not later* than ___

If this box is checked, the solution(s) or remedies to be provided by you to insure year 2000 Compliance by the date specified above are as follows:

_____
_____
_____
_____
_____

3. ❑ The product is warranted (by the manufacturer or by the seller to be Year 2000 Compliant. The warranty is attached to this form. (If you check this box, you must attach the warranty.)

Exhibit 5.3.1-2 Sample Vendor Letter (continued)

4. ❑ The functioning characteristics, and performance of the product are not affected by date or time sensitivity, and the functioning, characteristics and performance of the product will not be impacted by the century date change.

5. ❑ The product is **not** Year 2000 Compliant ad will not be made compliant.

6. ❑ Other options are available to make the product Year 2000 Compliant (e.g., maintenance agreements, upgrades, other). If this box is checked, the available options are as follows:

_____
_____
_____
_____
_____

PLEASE ACKNOWLEDGE THAT THE ABOVE INFORMATION IS CORRECT BY SIGNING IN THE SPACE INDICATED BELOW AND RETURN THE SIGNED SURVEY TO _____ BY FACSIMILE AT (_____)_____

ACKNOWLEDGED for _____ [insert name of Vendor]

By:_____
Signature of Vendor's Authorized Representative

Type or Print Name:_____

Title:_____

Date:_____

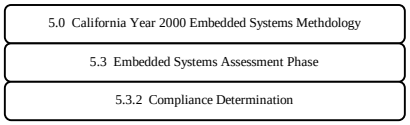
FAX SIGNED SURVEY TO:
_____
_____
_____
Phone: (____)_____
Fax: (____)_____

Vendor Responses. Review all vendor responses and flag all unclear, incomplete, or questionable responses for further research and analysis. Vendor product certifications should be carefully reviewed. It is important to note that different test environments cause different test results, and although a system may be deemed compliant for certain environments, it may not be compliant in yours. Proper exercise of due diligence may exceed reliance on vendor certification and require examining vendor test data, procedures, and even requesting vendor-demonstrated testing.

When an e-mail response is received, make sure that it contains a vendor logo or other specific identifying method that ties the response directly to the vendor; make a hard copy, date-stamped print-out of the web-site data.

The site survey and vendor management activities are iterative processes, and as such will be performed throughout the Year 2000 effort to determine the best course of action. This is a crucial phase to use configuration and data management processes. As more data is collected from additional surveys, research, and vendor contact, it is essential to organize the information and document all communication with the vendor. It is also important to baseline the data. A wide variety of activities, including system upgrades, replacements, tests, and vendor responses can make a significant impact upon future decisions in regards to system and department remediation efforts. A structured method of documenting and monitoring change efforts will enable departments to complete remaining efforts in a more effective manner, thus increasing the probability of department-wide Year 2000 embedded systems compliance

5.3.2 Compliance Determination



Compliance determination requires the analysis of all available data, including vendor data and related system interfaces, resulting in a decision of system Year 2000 compliance, non-compliance, or indeterminate—needs further action.

> Definition: The term "Year 2000 compliant" is defined as the capability of a system, component, or product to perform its intended function or functions without interruption, malfunction, or performance degradation, including the loss, corruption, or generation of inaccurate data as a result of internal date/time computations relating to the transition from the years 1999 to 2000 and beyond, and including computations relating to the occurrence of leap years.

Segregate. Based on review of the information gathered on the system, the identified risk category (i.e. health and safety, environment), the system ranking (high, medium, low), the date sensitivity, and the date functionality, systems are segregated by those

that require no further action, and those that require determination of compliance. This is the time to review system utilization and pre-existing operation and maintenance plans and efforts. The system in question may be scheduled for retirement or may already be identified in the current year's budget for replacement. Obviously in the case of retirement, no further action is required. However, the system that is in the process of Year 2000-compliant replacement should be monitored and included in contingency planning should it not be ready or compliant in time.

Determine Compliance. The date-sensitive systems are reviewed for level of compliance based on all the information received. Systems are classified as compliant, non-compliant, or unknown. Systems that are determined compliant, but are categorized and ranked as department critical require compliance testing. Additionally, for those systems where vendor data is inconclusive, ambiguous, or not available, it is also highly recommended to perform compliance testing. Table IV shows a compliance matrix by risk category (as defined in the first phase, risk analysis) to assist in determining whether to perform compliance testing.

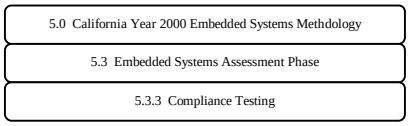
Table IV. Embedded Systems Compliance Matrix

		System Y2K Compliant?		
Risk Category	**Risk Ranking**	**If Yes:**	**Unknown:**	**If No:**
Health/Safety	H or M or L	Test all*	Test all* or remediate	Remediate
Environment	H or M or L	Test all*	Test all* or remediate	Remediate
Operations	H or M or L	Sample test or NFA	Test all* or remediate	Remediate or workaround
Public Confidence	H or M or L	NFA	Test sample, remediate, workaround, or ignore	Remediate, workaround, or ignore
Other	H or M or L	NFA	Workaround or ignore	Workaround or ignore

* Within department cost, volume and schedule constraints, in cases where there are multiple identical systems.

KEY: H = High
NFA = No Further Action
M = Medium
L = Low

5.3.3 Compliance Testing



Compliance testing is the testing of systems to determine whether it is Year 2000 compliant, non-compliant, or unknown. It is performed for many reasons: (1) lack of vendor response, (2) to verify system compliance (regardless of certification), and (3) to test system compliance for custom-developed systems for which there is no single vendor (system built in-house). The object of the test is to observe system performance subsequent to the Year 2000, using simulated dates. The test results will provide additional information to make a determination of system compliance, backup or disprove earlier statements or findings, and provide a heads-up, advanced view as to how severe or insignificant Year 2000 failures will be for the department.

Test Planning. Start planning test activities. Develop a comprehensive test plan and schedule; designate an overall test coordinator, and facility or functional area coordinators; and establish points of contact for all systems to be tested. Additional personnel involved in testing should include the system lead engineer, facility manager, chief engineer, support contractors, manufacturer field representatives, and QA.

Determine which systems will require compliance testing, the level of testing necessary, the environment, the test conditions, the resources, and the interfacing systems that may need to be included at some level of the system's testing. Each system to be tested should have an individual test plan.

As part of the individual test planning effort, develop a diagram of system interrelationships and review these with the system lead (including the interdependent system lead, if any) and the testing group to ensure that the complete system is addressed and understood. Discuss and document system operation schedules, availability of back-up, or parallel systems, and the impact of system testing on other system testing schedules.

Individual plans should include test specifications, test routines, test procedures, and system test schedules. Contact vendor/manufacturers for available system test procedures, operator manuals and coordination of test activities. If testing is performed on-site, make sure on-site testing personnel are prepared in the operation and servicing of the equipment to make necessary field corrections, as needed to ensure normal operations are not impacted.

Identify Testing Levels. Determine level of testing required for each system. There are a number of test levels that may be executed in the process of compliance testing, listed as follows:

1. Facility level. This is a test of multiple systems where system boundaries are crossed (internal and external interfaces). This test ensures that the multiple

systems supplying, relaying, or receiving information that contains dates/time are handling and interacting correctly. This level may be difficult to perform and may require dividing into meaningful segments.

2. System level. This is a test that stays within the system boundaries, assuring that the system handles time correctly and no incorrect actions occur.
3. Component (unit) level. This test consists of testing the stand-alone component; i.e., the remote sensor feeding data into a larger system.

The level to which these tests are performed is at the discretion of the department Year 2000 project leads. For systems that are complex, cross system boundaries, and whose failure will cause significant departmental impact, it is highly recommended to perform all levels of testing. However, this may entail a significant expense and effort, and should be recognized accordingly.

Test Considerations. Test plans should address the following questions:

- Where will the testing be performed?
- Will tests be performed on the actual installed equipment, on an identical backup system, in a laboratory test environment at the vendor facility?
- What are the impacts of testing in each environment?
- Can a representative system configuration be developed in a laboratory or at the vendor facility?
- Does the vendor have test procedures to use or test reports to compare results against?
- How does the system use the date? Does it receive the date externally? If so, how will this be duplicated in the lab or vendor test environment?
- Has testing been coordinated with personnel responsible for the interdependent systems?
- How many systems should be tested? Will the test sample results[4] reflect how all the systems in the population will behave?
- If the system testing occurs on the installed system and it fails, can the system be restored to the original state?

[4] Re-evaluate system function criticality and operational impacts when determining sample sizes for testing. There have been cases where two nominally identical devices have been tested and found to be compliant in one case, but not the other. It is possible that a supplier provided items that were not those ordered but met the operational specification. Detection of this may not occur until testing.

- What are the expected test results?

- How much time, cost and resources will this test effort require and what is available?

System test procedures should include many test scenarios involving dates (see Appendix E). Because some embedded systems function on cycles, their failure may not be obvious when the date changes over to January 1, 2000. They may 'rollover' on that date without impact, and the failure may happen when the next cycle occurs.

It is also important to understand that dates can be represented in many forms other than the standard mm/dd/yy format. Address and consider all of the possible date representation systems in use to ensure that date processing will produce correct dates before, across, and after the millennium for all intra-century and trans-century processing.

***Test Guidelines**:*

The following are test guidelines to consider before initiating any system compliance testing:

- Separate test scripts, test environments, and test cases from the operational systems where possible;

- Back up all data and software prior to commencing testing;

- Test core elements (the hardware/software platforms) prior to testing the application software;

- Remember interface data can corrupt (make non-compliant) a system that tested compliant;

- Ensure the test platforms are identical to the operational system when running tests on a test platform;

- Ensure all test cases are covered;

- Ensure all software modules are executed in testing the program suite;

- Re-test as necessary to validate test results;

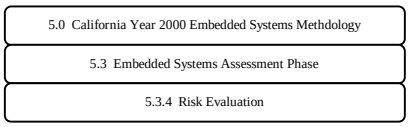
- Ensure that the test process does not erroneously expire software licenses or invalidate them because of copying or changing platforms. The test process may also result in the incorrect date logging of computer files and e-mail files.

It is very important to thoroughly plan and document this effort and have personnel who understand the system—such as system vendors, system leads, and operations

and maintenance employees—available to either perform the effort or provide assistance and guidance. It is also important to assure that staff members who work with interdependent systems are involved in the planning process. Thorough planning will mitigate unnecessary risk and ensure that the compliance test provides the most realistic scenario of the date change event.

Test Reporting. The results of the testing are reviewed, evaluated, and compiled into a report together with previously-gathered system status information (systems that were not tested) to provide a visual summary of department embedded systems compliance status. Systems identified as non-compliant or of indeterminate compliance status will then be analyzed for risk and prioritized for order of remediation in the next activity.

5.3.4 Risk Evaluation



The risk evaluation activity involves analysis of the non-compliant system failure scenario. This includes evaluation of the criticality of the system in relation to other systems (category ranking) within the same risk category (i.e., health and safety, environment); type of system risks and associated failure impacts; estimated cost of these failures; and vulnerability of the system (how it fails) and time to system recovery.

Re-evaluate System Category and Priority. In the risk analysis activity (phase one), systems were categorized according to health and safety, environmental, operational, public confidence, and other risk categories with the emphasis on first concentrating on identifying those embedded systems that contribute to departmental core mission functions and business operations (category ranking: high). During survey, vendor management, and compliance determination activities, additional information on each system was gathered and documented. The designated Year 2000 personnel, as a result of this effort, became more informed on the system's functionality and configuration. It is possible that upon further investigation, some systems will need to be re-defined in terms of importance to departmental core function. Because of these changes and the need for effective remediation activities, it is necessary to re-evaluate the non-compliant/indeterminate systems relative to other systems within the same risk category (category ranking).

For example, at first examination non-compliant elevator systems could all be categorized as a safety risk with a category ranking of high; failure resulting in possible injury/death. However, the failure of an elevator that services only two floors versus a twenty-five-floor elevator has a significantly different risk impact. The results of this re-evaluation would necessitate the re-ranking of the two-floor elevator down to a lower category ranking (i.e. high to low). This would result in the two elevators being placed at much different places on the priority list, and require some different remediation strategies for each.

Identify/Analyze System Risks and Impacts. This includes reviewing the entire system with interdependencies, if any, and identifying if there is a failure in any one component that causes a system Year 2000 failure, what type of risk is involved, and what impact results. Identify all the safety, health, operations, legal, resource, and public confidence impacts, and the likelihood of any or all ('worst case' failure scenario) of these occurring. An example of this risk identification might state the following: "failure could cause likely death, probable injury of staff and public, services unavailable for three days, lawsuits by staff and public families, significant equipment damage, and unfavorable media attention resulting in public distrust and loss of funding."

Estimate Failure Costs and Recovery Time. For the scenarios identified for each system, estimate the total failure cost. This may include equipment damage, medical, legal (attorney, court time and lawsuit costs), environmental (i.e. rebuilding, restoring costs), employee compensation, operational revenue loss, and funding reduction costs. These estimates should be reviewed and evaluated with department legal and financial staff to determine accurate and reasonable estimates of potential exposure.

Evaluate Date Change Vulnerability. Date change vulnerability refers to the extent the system will fail when the Year 2000 date change happens and the estimated time to recover. It is defined as follows:

Severe. The system/components identified will fail to operate normally without remediation. System recovery time is significant and not feasible.

Moderate. The system/components identified may fail to operate normally or may require manual intervention to re-establish normal operating conditions. Intervention may be required more than once per shift or machine operation cycle.

Minimal. The system/components identified may require manual intervention to re-establish normal operating conditions only once (i.e., manually resetting date/time to reinitialize the system). Further intervention will probably not be required.

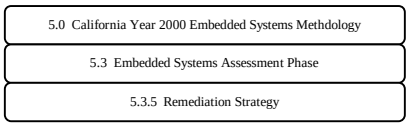
Identify the system configuration and assess each individual component in terms of vulnerability to the Year 2000 date change. Evaluate the system vulnerability classification selected based upon its impact on operations. For example, even if a system has manual resets (moderate) that can be performed, consider if operations can tolerate the system being down for any length of time.

This effort, together with the other risk assessments, will assist in making better decisions when determining system remediation priority and developing the remediation strategy.

Prioritize Systems. After assessing all the possible risks and impacts associated with the system failure, the project team should then work together with the departmental personnel to review findings and develop a "top-down" ranking of all systems

requiring remediation. This listing and background system information will be used to develop the remediation strategy. A prioritized list will ensure that the most critical and significant risk systems are handled first and remediation efforts are accomplished in a methodical way.

5.3.5 Remediation Strategy



The remediation strategy is the set of possible solutions that will best achieve system compliance within the time and cost constraints available. A system may have a combination of solutions, one for each non-compliant component, or will have one overall solution such as complete replacement. The most effective strategy for a particular system will take into account all the information gathered from previous efforts, and the time and effort required to implement the solution(s).

The remediation solutions are listed in Table V, below.

Table V. Embedded Systems Remediation Solutions

REMEDIATION SOLUTION	DESCRIPTION
Do Nothing	The system is Year 2000 compliant; is no longer used by the department; is deemed non-essential by the department; or is such that it cannot be upgraded or replaced.
Upgrade	A Year 2000 compliant version, release, or retrofit for the system is available. The cost, if any, is identified. Check existing lease, purchase, or maintenance agreements for legal obligations on the part of the vendor.
Replace	A Year 2000 compliant version or release is either not available or is undesirable due to cost, additional requirements, or schedule, but a functionally equivalent, Year 2000 compliant system is available from a vendor.
Workaround	A solution that provides a temporary or permanent Year 2000 solution such as manual date rollover action(s) or utilizing other means to achieve functionality until system can be fixed.
Undetermined	A responsible vendor could not be determined; often custom systems fall into this category. These require additional 'Special Handling' which entails further review and possible reverse engineering subject to cost/schedule.

To help evaluate the various solutions for each system, it is necessary to create a report that lists: (1) the system, (2) the particular remediation solution(s) that will

work for the system in question, (3) the estimated cost, time to implement (including testing), (4) resource requirements, (5) additional information that facilitates making the decision in favor/against using the indicated solution, and (6) the recommended solution. Start this evaluation in top order of the prioritized embedded systems list. The following Table VI provides an example of this report format.

Table VI. Remediation Strategy Report

Department: **System:** **Risk Category:** Environmental **Category Ranking:** Medium **Vulnerability:** Moderate				
Remediation Solution	**Cost** (including labor and tools)	**Time** (including time to test)	**Resources**	**Comments**
Replace	$23,000	12 weeks	3 people, 2 person-months	similar parts in stock; compliant
Upgrade	$20,000	8 weeks	3 people, 1 person-month	Vendor testing in process; completion: TBD
Recommendation: Upgrade embedded system. Alternative: Replacement.				

This example is for a system that was built and integrated by the vendor; therefore, there is only one 'system' listed. For systems that comprise several non-compliant subcomponents, the model will be much more complicated. The model will be evaluating a set of solutions and variables for each non-compliant subcomponent, documenting the interface solution, if applicable, and the associated solution schedule/time, in order to develop an overall system strategy.

Additional difficulties are encountered when evaluating the best strategy for a custom system. The effort to accomplish remediation may require reverse engineering the system. In addition to determining the 'fix', several elements need to be considered such as how to test, the impact of the testing if the system should crash, and the effort, time and cost to test the compliant embedded system in its operational environment to verify compliance and functionality. Only in the case of extremely complex, custom-made embedded systems, or embedded systems that are software intensive with operator interface, will replacement costs exceed the cost of re-engineering a system and implementing upgrades; therefore in most cases it is recommended to replace the system, if possible.

The results of preparing this report will identify an overall system strategy; the next step will be the detailed remediation planning, and obtaining the necessary funding and resources to implement the selected Year 2000 compliant solution.

Whether the system strategy is to upgrade, replace, or workaround, it is extremely important for the department to include conditions of conformance to Year 2000 compliance criteria in their contracts for these services. All new embedded systems contracts and purchase orders undertaken by departments must include sufficient guarantees of Year 2000 compliance, including leap year considerations, so no ambiguity remains concerning who bears the risk of loss in the event of failure. The department should utilize the Department of General Services to facilitate the development of Year 2000 contract language in all remediation contracts.

5.4 Embedded Systems Remediation Phase

5.0 California Year 2000 Embedded Systems Methdology
5.4 Embedded Systems Remediation Phase

The purpose of the remediation phase is to develop the remediation and contingency plans, implement these plans (correct Year 2000 deficiencies), demonstrate Year 2000 compliance through testing, and monitor systems through the Year 2000 date change to ensure continued system operation. The overall activity is depicted in Exhibit 5.4-1.

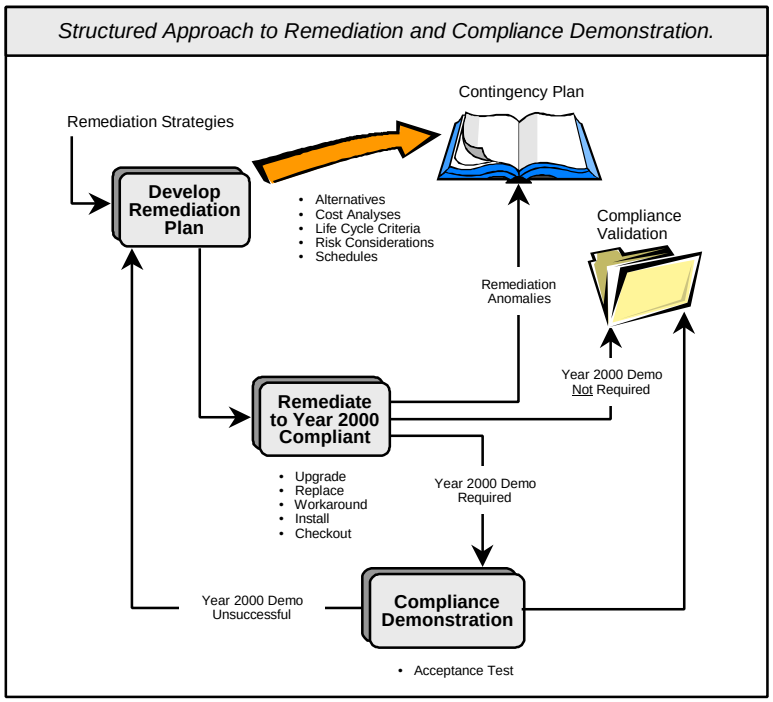


Exhibit 5.4-1 Embedded Systems Remediation Activities

5.4.1 Remediation Planning

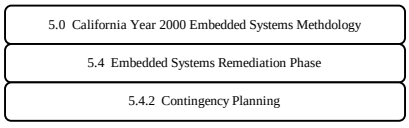
5.0 California Year 2000 Embedded Systems Methdology
5.4 Embedded Systems Remediation Phase
5.4.1 Remediation Planning

The remediation planning effort starts with reviewing in priority order, the system strategy, the schedule to support the strategy, and then determining what course of action is required to acquire/obtain/implement the solution(s) identified in the strategy. This involves developing system-level schedules, and creating detailed plans that address system procurement/replacement requirements, test specifications and procedures, resource requirements (tools and equipment), and personnel/vendors needed to support installation and test activities. As emphasized throughout this guide, interfacing systems need to be considered, especially in the remediation planning and implementation activities. From these activities, the department can then develop an overall remediation schedule.

Test Planning. The test planning activities are identical to those developed for compliance determination testing in Section 5.3.3. The difference between system compliance demonstration and system compliance determination testing may be that system-wide testing (including interfaces) was not performed, or only one set of tests was executed during compliance determination testing because of time or risk constraints. It is crucial that system-wide testing is planned for and performed during compliance demonstration to determine true system behavior and to execute these tests more than one time to ensure consistent results. As with compliance determination testing, the testing is designed to minimize and eliminate, where possible, any impact or potential impact to department operations. All test plans should include certain checkpoint milestones and a back-out procedure in the event the testing does not proceed as planned or fails in an unexpected manner.

Test Reporting. It is very important to identify processes for documenting all tests and test results to ensure that the remediation effort is conducted effectively and efficiently. This will enable the project team to easily identify where in the testing process any one system is; which systems need to be re-prioritized; where resources need to be added to meet testing schedules; and which systems simply will not meet the deadline and necessitate a workaround.

5.4.2 Contingency Planning



It is unlikely that all embedded systems will be addressed by January 1, 2000, and some validated Year 2000-compliant systems may not function properly. Therefore, it is essential that all departments develop contingency plans that address potential failure scenarios and determine how to best mitigate the impact of these failures within the cost and schedule constraints available.

Departments should strongly consider developing contingency plans for those high priority systems determined to be critical to department function (regardless of vendor certification or compliance status); systems which have no workarounds (if failure occurs); systems that compliance was indeterminate; and for those systems that did not successfully demonstrate Year 2000 compliance under initial testing.

The steps involved in contingency planning are as follows:

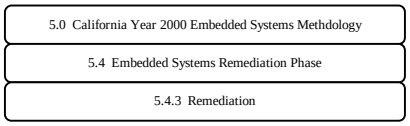
- identification of core mission functions and high-impact systems and priorities;
- identification of possible causes of failure, probability of failure; location of the problem, and problem solution;
- identification of interfacing systems that could cause system failure;
- definition of possible alternative actions, and criteria by which to choose the appropriate action(s) to be taken;

- determination of plan(s) for action should the failure occur, and the resources and personnel needed to support it;
- documentation and distribution of contingency plans to relevant personnel, and
- development and execution of training (in advance) that will prepare personnel for how the plan will work.

It is important to note that reliance on previously developed disaster-recovery processes and procedures may lead to continued business failure. Many of these plans rely on back-up facilities that may experience the same problems.

It is essential to have sufficient trained personnel and resources available, standing by, for the initial operational activities after January 1, 2000. Even the best testing process will not guarantee a problem-free system; being well prepared will minimize the impact on department operations.

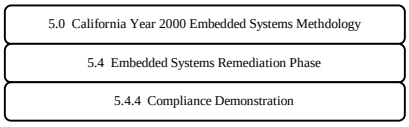
5.4.3 Remediation



Remediation actions may include system component replacement, complete system upgrade or replacement, incorporating operating system and application software changes in process controllers, or implementing a workaround plan. For most systems, remediation will involve installing the new system using normal installation test and checkout in accordance with the manufacturer's recommendations. It is recommended to initially perform installation and test activities at the vendor facility, if possible.

Departments may perform their own on-site remediation installation and test, or use a combination of vendors and consultants to do this, and provide the oversight, witness and documentation functions. It is important to use the system remediation plans and procedures and coordinate installation and test activities with all impacted parties. Installation and testing should be performed in a stand-alone mode (unit test) first, before installing with other system components. Meaningful segments of the system (other components and interfaces) should then be added and tested; thus helping to isolate the cause of failure, should it occur.

5.4.4 Compliance Demonstration



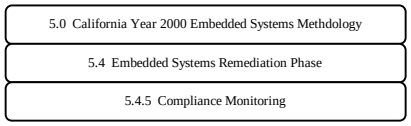
Compliance demonstration is also known as acceptance testing. It comprises all components of the system, including internal and external interfaces, tested together to determine total system compliance. Use system test plans and procedures, and as described earlier in remediation planning, create checkpoint milestones and a back-out procedure in the event the testing does not proceed as planned or fails in an unexpected manner. Coordinate testing with appropriate personnel, including interfacing system team members and system operation and maintenance personnel, to minimize system

operation impacts. As discussed in Section 5.3.3 Compliance Testing, system test procedures should include many test scenarios involving the different dates listed in Appendix E, and it is highly recommended that tests be rerun to validate test results, especially for high impact systems.

In the case that a system remediation fails testing, refer to the system's contingency plans where alternative and/or workaround solutions are contained and installation and test plans and procedures are defined. It is very important to document all test results, alternate solutions and system changes in the system configuration and test documentation. Failure to record this information could have significant operational impact if, during the actual date change, the new system configuration fails to operate correctly.

Provide test status frequently, as defined in the remediation planning process, so that efforts and resources are focused and effective, and risk is minimized as much as possible.

5.4.5 Compliance Monitoring



Starting on December 31, 1999, it is highly recommended to have personnel on-site (operations and maintenance and system lead personnel) prepared for possible system failure for those systems defined as core department functions or high-risk systems. Coordinate this effort with personnel responsible for interfacing systems, if applicable. Review contingency plans and procedures in advance, and make sure copies of these documents are on-site with the system.

There is no guarantee that testing will turn up every possible operation scenario, and the best risk mitigation is to be prepared for the worst situation by having backup plans and procedures.

Summary

The embedded systems Year 2000 effort is a challenge facing industry, government, and private citizens, alike, all over the world. It has a clearly defined schedule without delay. Starting now and using a structured process such as the California Embedded Systems Methodology, together with sound, implemented management practices will significantly improve the user's ability to successfully meet this challenge.

Section 6. California Embedded Systems Center

The DOIT established the California Embedded Systems Center (CESC) at www.cesac.com to serve as a repository of embedded systems Year 2000 compliance data for all state government entities. It was developed from an existing commercial database, and is intended to capture and serve as a repository for additional embedded systems compliance information as it is developed within the state. The use of the center is optional and will be free during the pilot phase.

6.1 Services Summary

The California Embedded Systems Center (CESC) is an on-line data repository service that is designed to work with the *California Year 2000 Embedded Systems Program Guide*. This service was established by the DOIT to assist state government entities in developing and implementing their Year 2000 embedded systems programs. Authorization to access this service is provided by the DOIT.

Data repository services available to the authorized user include use of the CESC database for storage of department embedded system information. This database was designed to capture the system data collected as the user moves through the California Year 2000 Embedded Systems Program methodology presented in the *California Year 2000 Embedded Systems Program Guide*. This saves the department or user the cost and time required to develop their own database. Using the program guide and the forms provided in the CESC web-site, the user has immediate access to the methods and forms necessary to conduct field investigations. Additionally, the CESC provides the user a standardized method to collect and store embedded system data.

Another service of the CESC repository is the query function, enabling the user to query the database for existing system or vendor information. The results of the query will be a listing of all the information available for that particular system or vendor.

A separately published web-site user's manual, the *California Embedded Systems Center User's Manual*, provides detailed instructions on how to use the web functions and the products delivered from each function. It is available upon request.

6.2 Access and Interface

Internet access to the CESC (www.cesac.com) will be authorized and controlled by the DOIT. User names and passwords will be provided by the DOIT by contacting the DOIT Project Manager at the DOIT main office number (916.445.5900). The CESC is designed to work with either Netscape or Microsoft Explorer, Version 3.0 and higher. Both Netscape and Microsoft Explorer are downloadable for free in these versions at the following Internet addresses:

Netscape:	http://www.netscape.com/download/selectplatform_1_1.html
Microsoft:	http://www.microsoft.com/msdownload/iebuild/ie4_win16/en/ie4_win16.html

For information on how to use the web-site, consult the *California Embedded Systems Center User's Manual* or call the toll-free CESC help desk at 1.800.433.1757. Help desk hours are from 8:00 a.m. to 5:00 p.m. (CA) Monday through Friday. If the line is busy, a message can be left by stating the specific request, contact name and phone number.

Glossary of Embedded Systems Terms

In an effort to increase communication among the departments and the DOIT, the following glossary of terms will be used as references for all publications, products, documents, and reports under the California's Year 2000 Embedded Systems Program.

California 2000 Office – The California 2000 Office is the DOIT organizational unit responsible for the California 2000 Program.

California 2000 Program – The California 2000 Program is a collection of Year 2000 services provided by the DOIT. It is comprised of multiple subprograms focused on particular types of systems, each susceptible to the Year 2000 problem:

Y2K SubProgram	System Type Addressed
California Year 2000 Program Guide	Traditional IT systems.
California Year 2000 Embedded Systems Program Guide	Embedded technology/microprocessor systems/non-IT systems, including telecommunications systems and wide area network infrastructure.
California Year 2000 Program Guide: Desktop Systems	Microcomputers and related network infrastructure, including file servers, local area networks, and desktop computers.
California Year 2000 White Paper: External Interfaces	External Interfaces coordination, synchronization and management issues.

The California 2000 Program services also include providing guidance where appropriate, promoting information-sharing, and facilitating analysis and reporting of associated Year 2000 costs and risks.

California Embedded Systems Center – An embedded systems data repository and technical assistance center established by the DOIT to assist state entities in performing their Year 2000 embedded system efforts.

California Year 2000 Embedded Systems Program – The set of activities performed by an organization which addresses the Year 2000 issues for that organization's embedded systems.

Embedded System – Embedded systems are microprocessor-based systems containing one or more "chips" or microprocessors used to control, monitor, communicate, or operate equipment. They are employed in a wide variety of systems such as communications systems, office equipment, traffic control systems, utility systems, security systems, elevators, medical monitoring equipment, environmental control systems and many others.

Embedded Systems Task Force – A forum of selected personnel empowered to represent their agencies' points of view in the development and operation of the Year 2000 Embedded Systems Program.

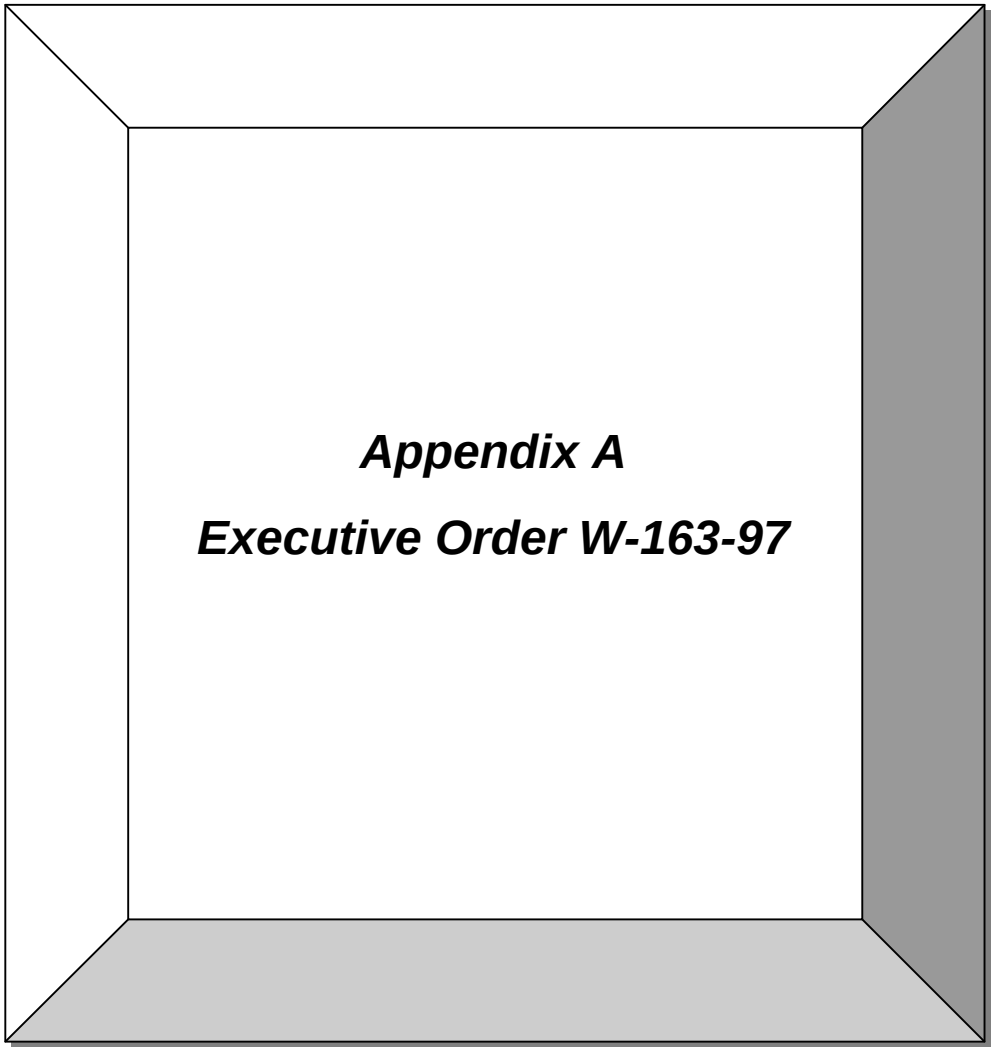
ES – Embedded systems.

ES Year 2000 Compliant – The term "Year 2000 compliant" is defined as the capability of a system, component, or product to perform its intended function or functions without interruption, malfunction, or performance degradation, including the loss, corruption, or generation of inaccurate data as a result of internal date/time computations relating to the transition from the years 1999 to 2000 and beyond and including computations relating to the occurrence of leap years.

ES Year 2000 Remediation – With respect to embedded systems, a set of activities which resolves the Year 2000 problems for the embedded system.

Y2K – An abbreviation for Year 2000.

Year 2000 Embedded Systems Project Manager – The individual empowered to lead, direct, and monitor Year 2000 embedded systems activities within an organization, and report to department management and the DOIT from a organization-wide perspective.



Appendix A

Executive Order W-163-97

EXECUTIVE ORDER W-163-97

WHEREAS, the State of California has a multi-billion-dollar investment in numerous information technology systems and equipment responsible for providing services and improving public safety for all Californians. and

WHEREAS, most computers and automated systems worldwide are threatened by the Year 2000 problem which, because previous date standards represented years with only two digits instead of four, fails to recognize dates beyond 1999; and

WHEREAS, the effectiveness of California's automated systems is at risk from the Year 2000 problem and, unless immediately addressed, a great many automated systems with mission-critical applications will be negatively impacted; and

WHEREAS, this Administration and the Legislature recognize the Department of Information Technology as the lead agency to coordinate and develop a comprehensive solution to the State's Year 2000 problem; and

WHEREAS, this Administration and the Legislature, through the Department of Information Technology's Year 2000 Program. have raised awareness of the Year 2000 issue and have proactively directed State agencies, departments, boards and commissions to assess and correct their Year 2000 problems; and

WHEREAS, the complex nature of the problem and the time necessary for California entities to detect Year 2000 flaws, devise solutions, and adequately test information systems make time of the essence;

NOW, THEREFORE, I, PETE WILSON, Governor of the State of California, bv virtue of the power and authority vested in me by the Constitution and statutes of the State of California, do hereby issue this order to become effective immediately:

1. Year 2000 solutions shall be a State priority. With due consideration for mandated initiatives, each agency shall defer commencing new computer projects until essential systems are Year 2000 compliant.

2. Each agency of the State shall be responsible to find and fix Year 2000 problems in its essential systems. in accordance with the Department of Information Technology's California 2000 Program, no later than December 31, 1998. Each agency shall also protect its essential systems from corruption by other systems which are not Year 2000 compliant. Agencies shall achieve compliance through existing resources.

3. State agencies shall not purchase new systems, hardware, software. or equipment that is not Year 2000 compliant or fails to contain Year 2000 contract language.

4. The Department of Information Technology shall continue to coordinate the State's information technology Year 2000 Program. The department shall:

a. Define Year 2000 compliance standards for the State.

b. Require quarterly reports from each State agency that is not Year 2000 compliant.

c. Analyze and validate any Year 2000 funding requests.

d. Provide Year 2000 progress reports quarterly to the Administration and the Legislature.

e. Foster solutions to the problems presented by embedded microchips in automated devices.

f. Address Year 2000 legal issues which may directly or indirectly affect State services.

g. Promote awareness of the Year 2000 problem to California public entities and private industry and underscore the need to proactively implement solutions.

5. Agencies shall report to the Department of Information Technology that information which the department may require.

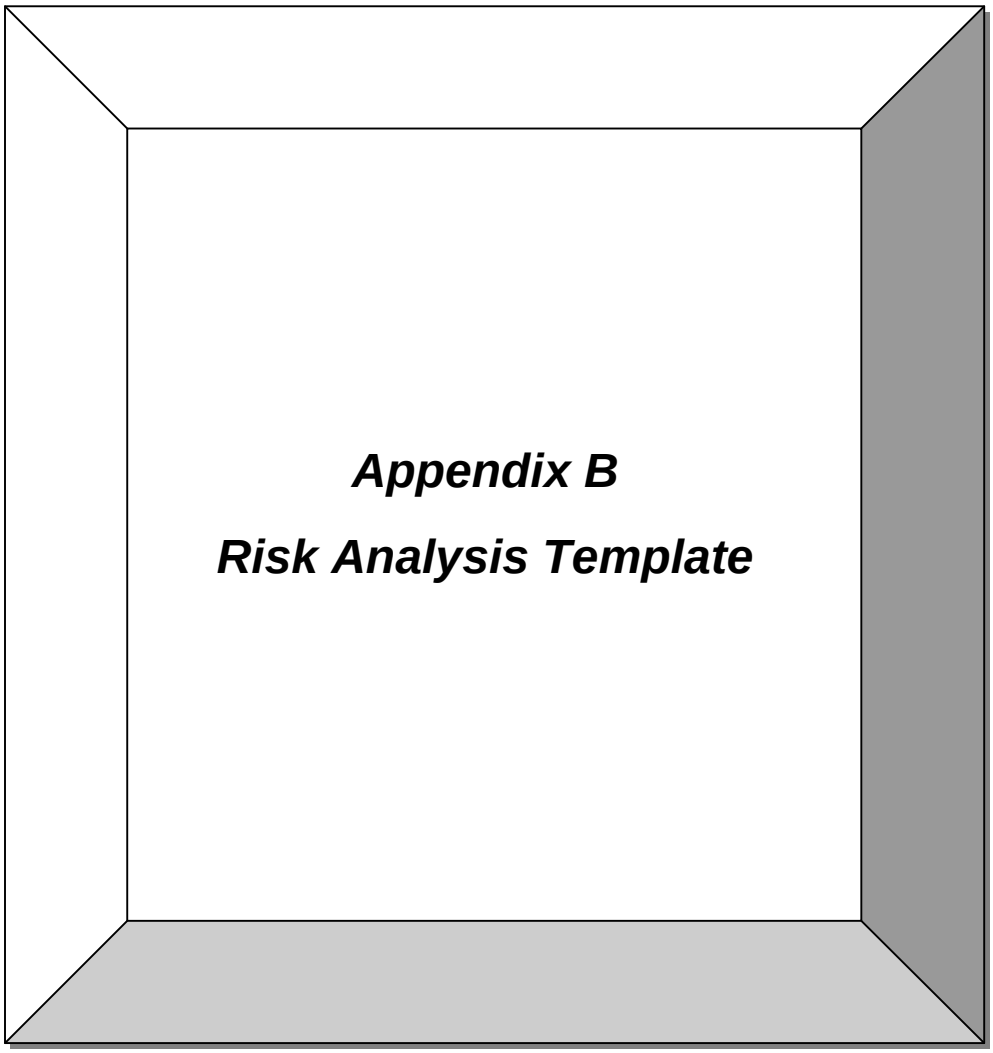
6. Unless subsequently extended, this Executive Order shall sunset June 30, 2001.

IN WITNESS WHEREOF I have hereunto set my hand and caused the Great Seal of the State of California to be affixed this 3rd day of October 1997.

Governor of California

ATTEST:

Secretary of State



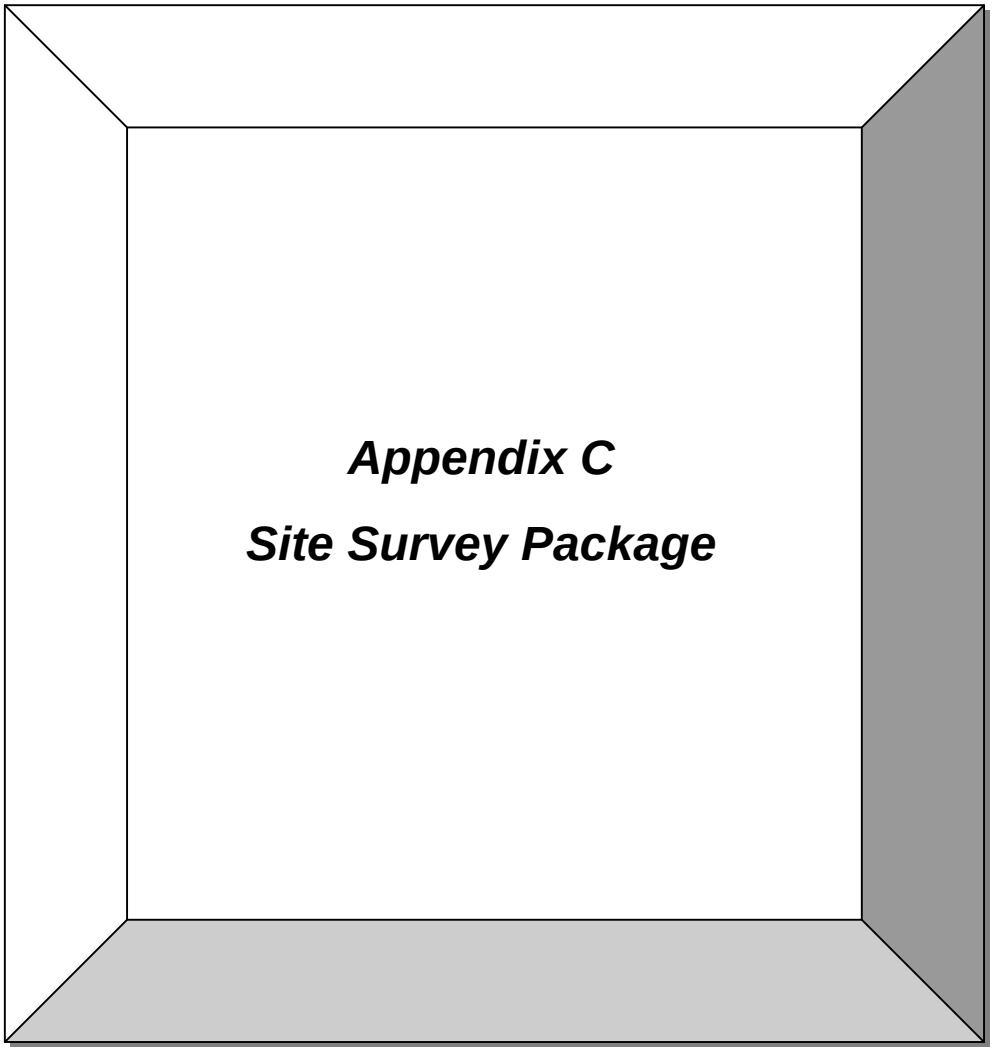
Appendix B

Risk Analysis Template

Risk Analysis Template

Department Name:	
Division/Section:	
Survey Date:	
Contact Person:	
Phone:	

Risk Category		**Category Ranking**			
No.	**Title**	**Total Systems**	**High**	**Medium**	**Low**
1	Health/Safety				
2	Environment				
3	Operations				
4	Public Confidence				
5	Other				
Total Embedded Systems					



Appendix C

Site Survey Package

Site Survey Form Guidelines

Forms Package Overview:

The site survey forms package consists of five forms, three of which will be used only once for each facility surveyed. Multiple copies of either of the two remaining forms will typically be required for each survey. The following paragraphs provide descriptions of the objectives for each form and the specific criteria for its use.

1. Form 1 – Site Survey Package Cover Sheet

A Site Survey Package Cover Sheet is completed for each individual facility surveyed. The five forms in the package will generally be completed by the department's Year 2000 Embedded Systems Project Office and provided to the members of the survey team as a means of coordination. All fields on this form are self-explanatory, with the following two exceptions:

1. **Facility Acronym Field:** This acronym will be used on all other forms in the package as a uniform, shorthand method of identifying the facility to which the other forms relate. If not assigned by the department's Year 2000 embedded systems project office, it will be defined by the members of the survey team and used consistently on all forms.
2. **Initial Meeting Time Field:** This field identifies the time at which the initial meeting is to occur between the members of the survey team and the representatives of the facility staff. In those instances where multiple facilities are to be surveyed, at a single location and with the same Points of Contact, this field should be completed only for the first scheduled facility to be surveyed.

2. Form 2 - Facility Systems Master Checklist

A Facility Systems Master Checklist will be completed by the survey team for each facility surveyed. The intent is that this form will be completed during the initial coordination meeting between the survey team and the members of the facility staff. Its purpose is to initially establish a master checklist of the specific system types within the facility for the purposes of planning and conducting the survey. At the completion of the survey, the collected data is compared to the Master Checklist to ensure that all required facility systems have been adequately covered.

Facility/Date/By: The first entry line on the form is self-explanatory. Transfer the Facility Acronym from the package cover sheet to this field. The date and the name of the person completing the form are entered in the two remaining fields on the line.

The form contains four columns of information, described as follows:

System Category and Type: lists various facility systems that are typically of interest for the purposes of this type of survey.

System Codes: lists specific System Codes that must be used when entering data on the remaining two types of forms contained in the package. **It important to use only these codes!** In the event that an applicable system code is not listed, use "OTH" as the system code when entering data on the remaining two types of data forms and further identify the system in the "Comments" section of the form.

Quantity or N/A: Each line in this column of the form should contain either an "N/A" to indicate that system type is not present in the facility, or a specific number (e.g. 1, 2, 3, etc.). In some cases a single facility will have more than one system of a given type (e.g. Access Control Systems). It is therefore essential to be aware of this fact to ensure that all applicable systems of a given type are properly surveyed and documented.

Comments: Use the comments section to document the needs of the survey team, or to provide clarification to the Analysts.

Except under very unusual circumstances, only one of the "Facility Systems Master Checklist" forms (Form 2) should be required for an individual facility.

3. Form 3 – System Survey Master List

The System Survey Master List is used to account for and summarize the survey results, estimated risk levels, and date sensitivity for each of the system types identified on the "Facility Systems Master Checklist." The summary data needed to complete this form is derived from information contained on the "Site Survey Forms" (Form 4). Thus, the completion of the necessary "Site Survey Forms" are a prerequisite for the subsequent completion of Form 3.

Multiple copies of Form 3 will typically be required for each facility surveyed. Accordingly, page number and total page information should be included as provided for at the bottom, right-hand corner of the form.

Prior to concluding a survey, this form is compared to the items identified on the Master Checklist (Form 2) to ensure that the requisite data has been collected both for each of the applicable system types and for the indicated number of systems within each type. The entries on this form are, in turn, supported by the detailed data that is contained on the Site Survey Form (Form 4), covered in the next section.

Facility/Date/By: The first entry line on the form is self-explanatory. Transfer the Facility Acronym from the package cover sheet to this field. The date and the name of the person completing the form are entered in the two remaining fields on the line. As will be noted, the form contains six data columns: The footnotes at the bottom of the form provide ready-reference guidelines regarding the first three columns on the form; however, each of the columns will also be addressed in more detail here.

System Code: Each row of this column should contain a valid System Code, as derived from Column 2 of the Master Checklist form. In the event that multiple components of a given system are being reported, repeat the System Code on as many rows in Column 1 as necessary. The component can be further identified in Columns 3 and/or 6, but it is important to retain its relationship to the overall system being reported against.

Sequence No.: This column is for use when multiple, non-identical systems of the same primary type are encountered within a facility; e.g., two separate and non-identical Access Control Systems within a single facility. Multiple occurrences of identical systems are handled differently, as described below, and do not require the use of Sequence Numbers. Sequence Number assignments are based on the information contained in Column 3 of the Master Checklist form and are made by the members of the survey team as a means to explicitly identify the specific system being reported on. Thus, if there are two separate Access Control Systems in the facility, the number "2" should have initially been entered in Column 3 of the Master Checklist (Form 2), in the row containing the "AC" System Code. The use of Sequence Numbers will, however, depend on which of the following two sets of conditions are applicable to the system in question:

Case 1 – Non-identical Systems of the same type: In the case where two systems are determined to be non-identical, both would be reported against a system code of "AC" in Column 1, but a Sequence Number of "1" would be assigned to one system and a Sequence Number of "2" to the other. In this way, the total number of systems of this type can be properly accounted for and reconciled against the quantity indicated on the Master Checklist.

Case 2 - Multiple Identical Systems: In the case where two systems were determined to be identical, in terms of the components used, but not necessarily the populations of each component (e.g., badge readers), then the system would only be reported once. In this case, Sequence Numbers would not be used; however, an entry must be included in the "Comments" field of the row to indicate the number of identical systems covered by the single report. This notation in the "Comments" field will enable the number of systems reported to be reconciled against the number indicated on the Master Checklist.

System/Component Name: a descriptive textual name for the System/Component being reported. In the case of multiple systems of a given type where Sequence Numbers are used, some textual reference should be used to distinguish each system. In the case where a System Component is being reported against a higher-level System Code, use this field to explicitly identify the component type.

Risk Category: Assign the appropriate Risk Category for each system, related to the type of impact resulting if the system in question fails to perform correctly. These are defined as follows:

a	Health and Safety
b	Environment
c	Operations
d	Public Confidence
e	Other

Date Sensitive: Categories for Date Sensitivity are defined as follows:

Category "Y": The item has been determined to be date sensitive, or has a reasonable expectation of exhibiting date sensitive characteristics.

Category "?": The item may exhibit date-sensitive characteristics, but additional analysis and/or research will be required in order to make a firm determination.

Category "N": The item has been determined not to, or to be extremely unlikely to exhibit date-sensitive characteristics.

Category "NF": The item has been explicitly been determined not to exhibit any possibility of date-sensitive behavior.

Comments: In general, the "Comments" column is primarily for the use of the survey team, either for their own purposes, or to convey specific information to the data analysts. There is, however, an exception as follows:

> **Exception #1:** This exception is addressed above in the discussion regarding Case 2, Multiple Identical Systems, where Sequence Numbers are not used: "however, an entry must be included in the Comments field of the row to indicate the number of identical systems covered by the single report. This notation in the comments field will enable the number of systems reported to be reconciled against the number indicated on the Master Checklist."

4. Form 4 – Site Survey Form

The Site Survey Form is used to record and document data for specific systems and components within the facility being surveyed. It is designed to acquire essential data pertaining to a wide variety of system types in a compact, efficient format, and to minimize the necessity for entering redundant information wherever practical. It is extremely important that all data is entered as ***completely*** and ***legibly*** as possible in order to avoid errors during the data entry process, and to minimize the required efforts on the part of the data analysis personnel who must both interpret the data and perform the necessary follow-up activities with the vendors. To assist in tracking and managing site survey forms, a page reference format (e.g., page 1 of 8) is provided for survey teams to complete. It is highly recommended that this field is utilized.

Blank data fields: Blank data fields on completed forms, are considered to represent data items that are pertinent to the system/component, but which were not available at the facility being surveyed. As all data fields will not be relevant to all systems, line through the unrelated sections or enter "N/A" in the data fields to provide the analyst with an explicit indication that these fields are not applicable to the system/component being documented.

The following discussion of the use of the "Site Survey Form" addresses each of the form data fields:

Facility/Date/By: The fields on this line are self-explanatory, and must be consistent with the information entered on Forms 1-3.

System Code: The appropriate system code from Column 2 of the Master Checklist form. In the event that the item being reported is a component of a larger system, but does not itself have a defined system code, use the code (and sequence number, if applicable) for the system of which this item is a part and identify this item in the "Description" field on line 3 of the form. Use the "OTH" system code only for an item that is not part of a larger system and for which an applicable system code is not supplied.

Sequence No.: This column is for use when multiple, non-identical systems of the same primary type are encountered within a facility; e.g., two separate and non-identical Access Control Systems within a single facility. Multiple occurrences of identical systems are handled differently, as described below, and do not require the use of Sequence Numbers. Sequence Number assignments are based on the information contained in Column 3 of the Master Checklist form and are made by the members of the survey team as a means to explicitly identify the specific system being reported on. Thus, if there are two separate Access Control Systems in the facility, the number "2" should have initially been entered in Column 3 of the Master Checklist (Form 2), in the row containing the "AC" System Code. The use of Sequence Numbers will, however, depend on which of the following two sets of conditions are applicable to the system in question:

Case 1 – Non-identical Systems of the same type: In the case where two systems are determined to be non-identical, both would be reported against a system code of "AC", in Column 1, but a Sequence Number of "1" would be assigned to one system and a Sequence Number of "2" to the other. In this way, the total number of systems of this type can be properly accounted for and reconciled against the quantity indicated on the Master Checklist.

Case 2 - Multiple Identical Systems: In the case where two systems were determined to be identical, in terms of the components used, but not necessarily the populations of each component (e.g., badge readers), then the system would only be reported once. In this case, Sequence Numbers would not be used; however, an entry must be included in the "Comments" field of the row to indicate the number of identical systems covered by the single report. This notation in the "Comments" field will enable the number of systems reported to be reconciled against the number indicated on the Master Checklist.

Subsystems: Mark the appropriate box. If the system identified has subsystems, mark "yes" and define the subsystem(s) and their location(s). A separate site survey form should be filled out and attached to the "master" system survey form.

Description: A concise textual description of the System, or System Component, to which the form data applies; this is required information and must be filled in.

Manufacturer: The name of the manufacturer, or the primary provider of the system or component being reported; this is required information and must be filled in.

Model #: The model number of the item, as defined by the manufacturer; this is required information and must be filled in.

Serial #: The manufacturer's serial number for the item (if available). As a general rule, do not attempt to record individual serial numbers for high populations of identical items such as video cameras and VCR's. In these cases, the manufacturer and model number is sufficient, but ensure that all combinations of these are reported.

Population: This field only applies when multiple identical items (i.e., differing only in Serial Number) are being reported. In this case record the total number of such items in this field.

Manufacturer Address: Enter the indicated data if available; otherwise leave blank.

Date Sensitive: Categories for Date Sensitivity are defined as follows:

Category "Y": The item has been determined to be date sensitive, or has a reasonable expectation of exhibiting date sensitive characteristics.

Category "?": The item may exhibit date-sensitive characteristics, but additional analysis and/or research will be required in order to make a firm determination.

Category "N": The item has been determined not to, or to be extremely unlikely to exhibit date-sensitive characteristics.

Category "NF": The item has been explicitly been determined not to exhibit any possibility of date-sensitive behavior.

Risk Category: Assign the appropriate Risk Category for each system, related to the type of impact resulting if the system in question fails to perform correctly. These are defined as follows:

a:	Health and Safety
b:	Environment
c:	Operations
d:	Public Confidence
e:	Other

Interdependent Systems: These are the internal or external interfaces that support the system in question. Differentiated from subsystems or components of the main system, these are separate systems that provide input into the system, or to which the system provides data outputs. If "yes" is marked, provide system name, location, and point of contact name and phone number.

Describe impact of failure due to non-compliance: Describe in concise textual terms the impact of such a failure, as related to the risk-level impacts defined for Form 3.

System Vendor or Support Contractor Data: Enter the indicated data if available; otherwise leave blank.

System Vendor or Support Contractor Data: If available, enter the indicated data for the System Vendor and/or the current system Support Contractor.

Control Computer Data (if applicable)**:** For those instances where the system being reported on is controlled by a computer or workstation, enter as much of the indicated data as is practical.

Comments Lines: The survey team uses this space to record additional information pertinent to convey to the Data Analyst personnel, and/or contributing to the overall objectives of the survey.

5. Form 5 – Utilities Suppliers

Complete only one "Utilities Suppliers" form for each facility surveyed. This form is used to the identify each of the companies that provide critical utilities services to the facility and should include Point of Contact information if available. The individual fields on this form are self-explanatory, and are not detailed individually.

California Year 2000 Embedded Systems Program
Facility Systems Master Checklist

Form completed by:	

Date:	

Department:	
Facility Owner:[5]	
Facility Name:	
Address:	
Facility Acronym **(used on survey forms):**	

Contact Information	
Chief Engineer:	
Phone:	
Facility Manager:	
Phone:	
Other Contact:	
Phone:	
Initial Meeting Time:	

[5] Facility Owner: The state/department may own the facility or it may be leased. This information has significance when a leased building has facility-related embedded systems requiring Year 2000 remediation actions**.**

Form #2

California Year 2000 Embedded Systems Program
Facility Systems Master Checklist

Facility: _____ **Date:** _____ **By:** _____

SYSTEM CATEGORY AND TYPE	System Codes	Quantity or N/A[6]	Comments
A. Fire/Life/Safety Systems			
Fire Detection and Alarm	**FA**		
Smoke Detection	**SD**		
Fire Suppression (Halon/Gas)	**FSH**		
Fire Suppression (Pre-action Sprinklers)	**FSS**		
Intercom/PA	**IC**		
B. Building Control Systems	**BCS**		
Lighting Controls	**LC**		
Landscape/Irrigation Controls	**LSC**		
Signs/Sign Clocks	**SGN**		
Parking Control Systems	**PRK**		
Under-floor Liquid Leak Detection	**ULD**		
C. Security/Surveillance Systems			
Access Control Systems	**AC**		
Video Surveillance Systems	**VS**		
Vault Locking Systems	**VLT**		
Intrusion Alarm Systems	**IAL**		
D. Electrical Systems			
Standby Generator Systems	**SBG**		
Uninterruptible Power Systems	**UPS**		
Battery Monitoring Systems	**BTM**		
Electrical Switchgear	**ESG**		
Automatic Transfer Switch	**ATS**		
Emergency Power Off	**EPO**		
Power Distribution Units	**PDU**		
E. Mechanical Systems			
HVAC Controls	**HVAC**		
Chiller/Compressor Controls	**CMP**		
Thermostats/Digital	**DTS**		
Humidification Systems	**HUM**		
Air Filtration	**FIL**		
VFD/Motor Controls	**VMC**		
Storage Tank Level Monitor Systems	**TLM**		
Storage Tank Leak Detection Systems	**TLD**		
F. Transportation Systems			
Elevator Controls	**ELV**		
Escalator Controls	**ESC**		
Vertical Lift/Conveyor Systems	**VLC**		
G. Other (Specify in Comments)	**OTH**		

[6] Total quantity of systems of the indicated type; otherwise enter "N/A" if not applicable to this facility.

California Year 2000 Embedded Systems Program
Facility Systems Master Checklist

Facility: _____ **Date:** _____ **By:** _____

System Code[7]	Sequence No.[8]	System/Component Name[9]	Risk Category a,b,c,d,e [10]	Date Sensitive (Y/?/N/NF)	

[7] Use System Codes as defined by the Facility Systems Master Checklist Form
[8] Use only when multiple systems of the same type exist within a single facility (used to differentiate between like systems for data collectio
[9] Descriptive name. See Guidelines for Forms 3 and 4 for details.
[10] Risk Categories: (a) Health & Safety; (b) Environment; (c) Operations; (d) Public Confidence; (e) Other;
See Site Survey Form Guidelines or California Year 2000 Program Guide for definition.

Form #4

California Year 2000 Embedded Systems Program
Facility Systems Master Checklist

Facility: _____ **Date:** _____ **By:** _____

System Code: _____ **Sequence No.:** _____

Are there subsystems? ☐ **Yes** ☐ **No** **If yes, list below.**
Description: _____ Location: _____
Description: _____ Location: _____
Fill out separate Site Survey Form for each subsystem and attach to this form.

Description[11]**:** _____

Manufacturer[1]**:** _____

Model #:[1] _____ **Serial #:** _____ **Population:** _____

Manufacturer Address: _____

Telephone: ( ) _____ **POC:** _____

Date Sensitive ? (Y/?/N/NF) _____	**Risk Category:**	☐ Health & Safety	Any interdependent systems?
If yes, what function? *Circle one*	*Check one*	☐ Environmental	☐ **Yes** ☐ **No** **If yes, list below**
Passive		☐ Operational Impact	Name:
Active		☐ Confidence in Gov.	POC:
Cyclical		☐ Other	Phone:
Unknown			

Describe impact of failure due to non-compliance: _____

System Vendor	**Support Contractor**
Name:	**Name:**
Address:	**Address:**
Phone:	**Phone:**
POC:	**POC:**

Control Computer Data (if applicable)**:**

Manufacturer: _____ **Model #:** _____ **Serial #:** _____
Operating System: _____ **Version #:** _____ **PC Clone ?** **Y** or **N**
Processor Type: _____ **BIOS:** _____
Software Title: _____ **Version #:** _____
Software Vendor: _____ **Telephone:** ( ) _____
Vendor Address: _____

Comments:

[11] **In order to effectively proceed with vendor management activities, data must be gathered for these fields.**

California Year 2000 Embedded Systems Program
Facility Systems Master Checklist

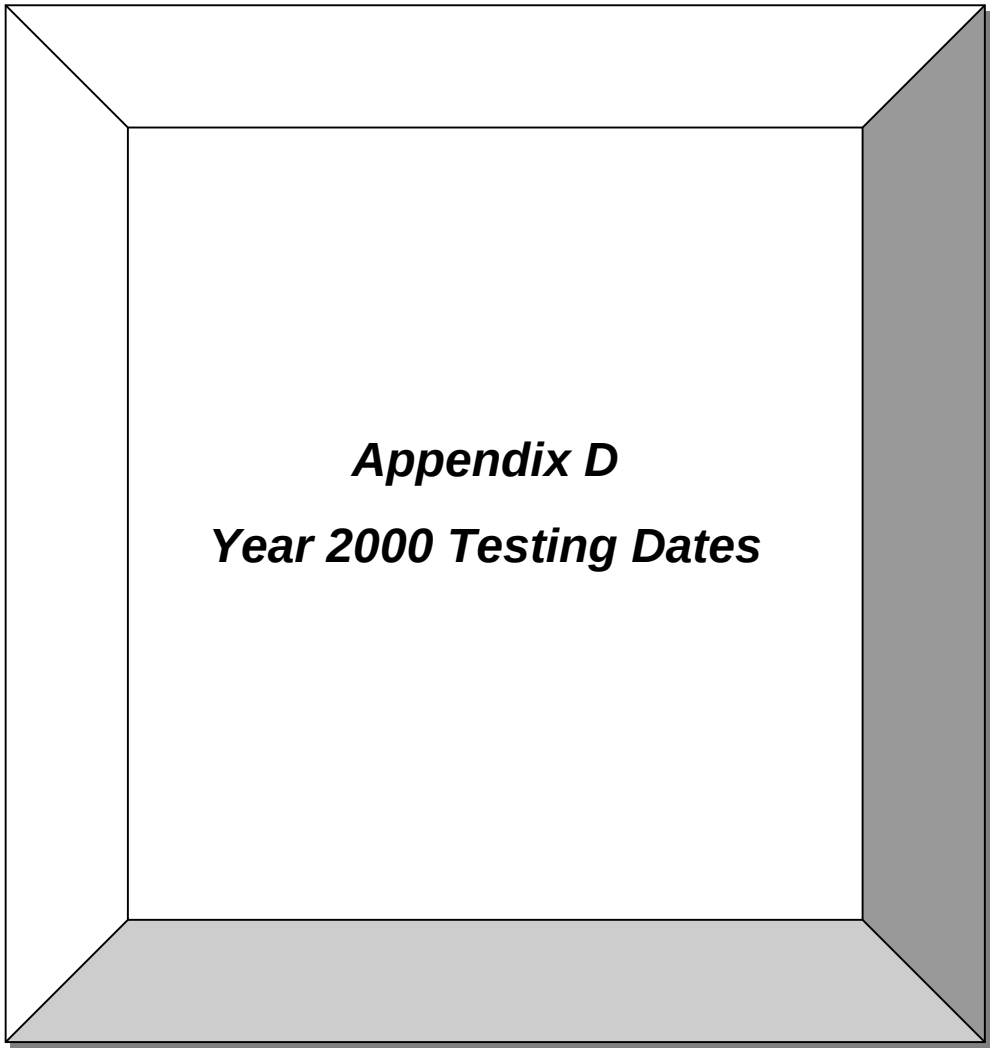
Facility: _____ **Date:** _____ **By:** _____

Electric Power	
Name:	
Address:	
POC:	
Phone:	

Natural Gas	
Name:	
Address:	
POC:	
Phone:	

Water	
Name:	
Address:	
POC:	
Phone:	

Other	
Name:	
Address:	
POC:	
Phone:	



Appendix D

Year 2000 Testing Dates

Date	Year 2000 Relationship
January 1, 1999	The first date using "99" in the year field. May impact files using "99 as a flag for special handling of the data.
September 9, 1999	The date that may be stored as 9/9/99 which may be a special processing event flag (i.e., end of a keep forever indicator or a delete all indicator).
December 31, 1999	The last date using "99" in a two-byte field. For systems that "look forward" as part of date processing, this date may cause errors when the date is used with the "00" of the Year 2000.
January 1, 2000	The first date using "00" in a two-byte field. For systems that "look back" as part of the date processing, this date may cause errors when the date is used with the "99" of the year 1999. The "00" representation may also be considered an event flag to trigger some special type of processing within a system. The first date where 24-hour look-forward processing in a system may cause an error due to manipulation of "00" in computing the look-ahead event (i.e., it may cause a calculation error where both dates are "00").
January 2, 2000	The first date where 24-hour look-back processing in a system may cause an error due to manipulation of "00" in computing the look-backward event.
February 28, 2000	The first date that is the day just before the first leap day of 2000. The date processing significance is to ensure a correct date rollover to February 29, 2000.
February 29, 2000	The first date that is a leap day in the Year 2000. The significance is the capability of a system to correctly roll over to this date.
March 1, 2000	The first date that occurs after the first leap day in the Year 2000. The significance is the capability of a system to correctly rollover to this date after having successfully rolled to February 29, 2000.
December 31, 2000	The last date using "00" in a two-byte year field. For systems that "look forward" as part of date processing, this date may cause errors when the date is used with the "01" of the Year 2001.
January 1, 2001	The first date using "01" in a two-byte field. For systems that "look back" as part of date processing, this date may cause errors when the date is used with the "00" of the Year 2000.

Date	Year 2000 Relationship
February 28, 2001	The first date that is not followed by a leap day. The significance of this date is the capability to correctly rollover to March 1, 2001, and not erroneously roll to the incorrect date of February 29, 2001.
February 29, 2001	The first invalid leap day of the millennium. The significance of this date is the capability of the system to correctly detect that this is not a leap day.
March 1, 2001	The first date that follows the first potential erroneous leap day. The significance of this date is the capability of a system to correctly rollover from February 28, 2001, to this date without an intervening and erroneous leap day.
February 28, 2004	The first date that is followed by a leap day that is not the special 4-year/400-year leap day calculation. The significance of this date is the capability of the system to correctly rollover to February 29, 2004, and not erroneously rollover to the incorrect date of March 1, 2004.
February 29, 2004	The second valid leap day of the millennium and the first leap day that is not the special 4-year/400-year calculation. The significance of this date is the capability of the system to correctly rollover to this date from February 28, 2004.
March 1, 2004	The first date that occurs after the second leap day in the Year 2000. The significance of this date is the capability of the system to correctly rollover to this date from February 29, 2004.